PowerShell Lecture Notes - 3

Topic: Reconnaissance And Scanning

Course: Hands-On Penetration Testing With Powershell
Date: 18-03-2024
Professor/Speaker:

Questions	Notes
Reconnaissance	-> Gathering of relevant information before taking action.
Powershell Cmdlets	• Get-ADGroupMember : Fetched members of active directory group. • gwmiWin32_Group : All users involved in administrative roles. • systeminfo : Information about OS. • netdom /query dc : Queries the domain for the list of domain controllers • gci c:\ -Include *pass*.txt, *cred* -File -Recurse -EA SilentlyContinue : Will scan C: drive for all files having "pass" or "cred" in their filenames. • Select-String -Pattern "Keyword" : Can be used to search for keyword in a file or text block. • hostname : Prints host name.
Scanning	-> Port and Network scanning is important for penetration testing. -> Usually enterprises keep ports of important computers such as servers closed by default.
Sensitive File Accessing	-> Files such as credentials or files with important informations.