

PowerShell Lecture Notes - 4

Topic: Active Directory

Course: Hands-On Penetration Testing With Powershell

Date: 19-03-2024

Professor/Speaker:

Questions	Notes
Credential Stealing	<ul style="list-style-type: none">-> Even when you're hacked in to a system, credential stealing is important because most probably the account which you used to hack in has low privileges, accounts with high privilege are more secure.
Client-Side Attacks	<ul style="list-style-type: none">-> Very frequently used.-> Payload : Some component of the attack which causes harm to the victim by exploiting vulnerabilities.-> Payloads are hidden in files using macros.-> Enabling of macro on client system is important.-> Attacking servers is not effective, so client-side attacking is better.
Brute Force Attacks	<ul style="list-style-type: none">-> Trying all possible passwords on various usernames, to get login access.