PowerShell Lecture Notes - 6

Topic: PowerShell And Metasploit

Course: Hands-On Penetration Testing With Powershell
Date: 21-04-2024
Professor/Speaker:

Questions	Notes
What Is Metasploit?	-> The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. -> Allows us to automate all stages of penetration testing.
Stages Of Penetration Testing	-> Information gathering -> Enumeration -> Gaining Access -> Privilege Access -> Maintaining Access -> Covering Tracks
Metasploit Meterpreter	-> It's a shell session, it has native support for powershell. -> It can use powershell import to load scripts locally into the system of penetration tester or attacker. -> You can attack machines w/o uploading such scripts on target systems.
Pass The Hash Attack	-> When we obtain hashes from target systems, using certain hash dumping tools and afterwards use such tools to inject obtained hashes on a local security authority subsytem service.