GitHub - Exploit-install/PSAttack-1: A portable console aimed at making pentesting with PowerShell a little easier.

By Jared Haight

Archived: 2026-04-02 12:40:57 UTC

PS>Attack 

A portable console aimed at making pentesting with PowerShell a little easier.

What is it

PS>Attack combines some of the best projects in the infosec powershell community into a self contained custom PowerShell console. It's designed to make it easy to use PowerShell offensively and to evade antivirus and Incident Response teams. It does this with in a couple of ways.

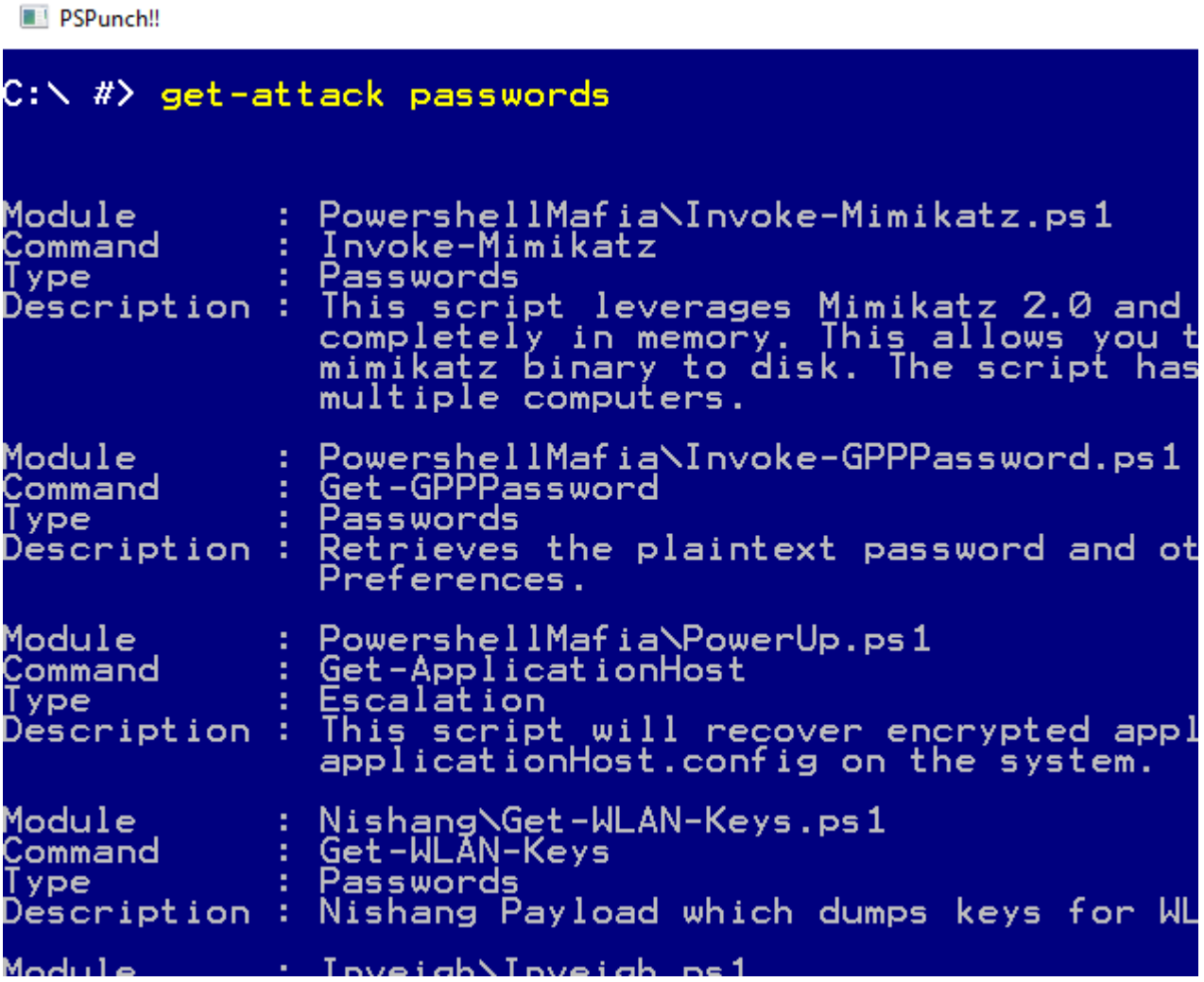
1. It features powerful tab-completion covering commands, parameters and file paths.
2. A custom command "get-attack" is included that helps you find the attack that you're looking for.
3. It doesn't rely on powershell.exe. Instead it calls powershell directly through the .NET framework. This makes it harder for enterprieses to block.
4. The modules that are bundled with the exe are encrypted. When PS>Attack starts, they are decrypted into memory. The unencrypted payloads never touch disk, making it difficult for most antivirus engines to catch them.

PS>Attack contains over 100 commands for Privilege Escalation, Recon and Data Exfilitration. It does this by including the following modules and commands:

- Powersploit
  - Invoke-Mimikatz
  - Get-GPPPassword
  - Invoke-NinjaCopy
  - Invoke-Shellcode
  - Invoke-WMICommand
  - VolumeShadowCopyTools
- PowerTools
  - PowerUp
  - PowerView
- Nishang
  - Gupt-Backdoor
  - Do-Exfiltration
  - DNS-TXT-Pwnage

    - Get-Infromation
    - Get-WLAN-Keys
    - Invoke-PsUACme
- Powercat
- Inveigh

It also comes bundled with `get-attack`, a command that allows you to search through the included commands and find the attack that you're looking for.



You can find a list of commands included in PS>Attack here

How to use it

PS>Attack is available as a pre-compiled binary on the releases tab. No setup or install is required, you can just download it and run.

Another option is to use the PS>Attack Build Tool. The build tool handles downloading PS>Attack, updating the modules to the latest versions, encrypting them with a unique key and then compiling the whole thing. The end

result is a custom version of PS>Attack that has all the latest tools and a custom file signature thanks to the unique key.

Of course, you can also just clone the repo and compile the code yourself. You can use Visual Studio Community Edition to work with it and compie it.

Contact Info

If you have any questions or suggestions for PS>Attack, feel free to submit an issue or you can reachout on twitter or via email: jaredhaight `at` prontonmail.com

Gr33tz

PS>Attack was inspired by and benefits from a lot of incredible people in the PowerShell community. Particularly mattifiestation of PowerSploit and sixdub, engima0x3 and harmj0y of Empire. Besides writing the modules and commands that give PS>Attack it's punch, their various projects have inspired a lot of my approach to this project as well as my decision to try and contribute something back to the community.

A huge thank you to Ben0xA, who's PoshSecFramework was used to figure out a lot of things about how to build a powershell console.
