Pen Test Diary

Jumat, 25 Agustus 2017

PowerShell for Pen Testers

In truth I simply needed a place to store and sort all of the Powershell tools I find and thought it might be of use for others:

PowerShell Empire - Pure PowerShell post-exploitation agent.
Powertools - A collection of PowerShell projects with a focus on offensive operations. This contains both PowerUp (tool to assist with local privilege escalation on Windows systems) and PowerView (tool to gain network situational awareness on Windows domains) both of which were chosen as Raphael Mudge's favourite Powershell tools along with the next one:
PowerSploit - A collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment. PowerSploit is comprised of the following modules and scripts:
PoshSec - A framework for PowerShell and PoshSec scripts for network management, security, and maintenance.
UnManagedPowerShell - Executes PowerShell from an unmanaged process. With a few modifications, these same techniques can be used when injecting into different processes (i.e. you can cause any process to execute PowerShell if you want).
CrackMapExec - A swiss army knife for pentesting Windows/Active Directory environments
Nishang - PowerShell for penetration testing and offensive security.
Kautilya - Tool for easy use of Human Interface Devices for offensive security and penetration testing.
PSRecon - Gathers data from a remote Windows host using PowerShell (v2 or later)

PowerCat - Netcat: The powershell version.
WMIOps - Powershell script which uses WMI for various purposes across a network.
RWMC - Powershell - Reveal Windows Memory Credentials
PowerMemory - Exploit the credentials present in files and memory
PoshRat - PowerShell Reverse HTTPs Shell
WmiSploit - Small set of PowerShell scripts that leverage the WMI service, for post-exploitation use.
PoshNessus - PowerShell Module for automating Tenable Nessus Vulnerability Scanner.
PoshSecMod- PowerShell Module with Security cmdlets for security work
PowerShellArsenal - A PowerShell Module Dedicated to Reverse Engineering
PowerForensics - PowerShell digital forensics framework
PowerShell-AD-Recon - PowerShell Scripts I find useful
PoshShodan - PowerShell Module to interact with the Shodan service
PSPunch - An offensive Powershell console

di 00.27

Tidak ada komentar:

Posting Komentar

Masukkan komentar Anda...

Beri komentar sebagai: Google Accoun

Publikasikan Pratinjau

Posting Lebih Baru Beranda Posting Lama

Langganan: Posting Komentar (Atom)

Metasploit Cheat Sheets

Wireless Hacking WiFu

Applocker Bypass Technique

Packet Crafting

CREST CCT Application Exam

Windows Patch Management Strategies

Persistence

Lateral Movement

IPv6 for Pentesters
