

Listing 4: Get-AdminAccount.ps1

```
$computerName = $env:COMPUTERNAME
$computer = [ADSI] "WinNT://$computerName,Computer"
foreach ( $childObject in $computer.Children ) {
    # Skip objects that are not users.
    if ( $childObject.Class -ne "User" ) {
        continue
    }
    $type = "System.Security.Principal.SecurityIdentifier"
    # BEGIN CALLOUT A
    $childObjectSID = new-object $type($childObject.objectSid[0],0)
    # END CALLOUT A
    if ( $childObjectSID.Value.EndsWith("-500") ) {
        "Local Administrator account name: $($childObject.Name[0])"
        "Local Administrator account SID: $($childObjectSID.Value)"
        break
    }
}
```