Registry <https://os.cybbh.io/public/os/latest/004_windows_registry/reg_fg.html#_6_security>

ADS <https://os.cybbh.io/public/os/latest/005_windows_ads/ads_fg.html>

### 5.5 Critical Registry Locations

<https://learn.microsoft.com/en-us/sysinternals/downloads/psexec>

**Secure COPY**

scp -r /home/username/somedirectory andy.dwyer@10.50.20.2:C:\users\andy.dwyer\Desktop

scp -r andy.dwyer

<https://haydenjames.io/linux-securely-copy-files-using-scp/>

The HKEY\_CURRENT\_USER registry hive is a symbolic link to another registry subkey. What is the subkey that it is linked to?

**Get-LocalUser | select name, sid**

….Over 1000 is usually new user accounts

Figure out the manufacturer's name of the only USB drive that was plugged into this machine.

**reg query** HKEY\_LOCAL\_MACHINE\system\currentcontrolset\enum\usbstor

What is the value inside of the registry subkey that loads a single time when the "student" user logs on?

What registry subkey runs a single time, then deletes its value once the machine reboots?

What is the value inside of the registry subkey from registry\_basics\_9?

reg query HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\**runonce**

What is the value inside of the registry subkey that loads every time the "Student" user logs on?

reg query HKEY\_CURRENT\_USER\software\microsoft\windows\currentversion\run

**OR**

get-item registry::HKEY\_USERS\\*\software\microsoft\windows\currentversion\run

What is the value inside of the registry subkey that loads a single time when the "student" user logs on?

get-item registry::HKEY\_USERS\\*\software\microsoft\windows\currentversion\run**once**

C:\worm.exe

What suspicious wireless network, found in the registry, has this system connected to?

get-childitem "HKEY\_LOCAL\_MACHINE\software\Microsoft\windows NT\currentversion\networklist\profiles"

What suspicious user profile, found in the registry, has connected to this machine?

Examine the readme file somewhere in the CTF user’s home directory.

get-childitem -path C:\Users\CTF -include \*readme\* -recurse