### Lab - Dumping Wi-Fi Credentials Using netsh

**Overview**

In this short lab, you will learn how to you dump Credential dumping is said to be a technique through which username and passwords are extracted of any login account from the target system. It is this technique that allows an attacker to get credentials of multiple accounts from one person. And these credentials can be of anything such as a bank, email account, social media account, wireless networks.

This lab requires that you have a Windows machine that at one time connected to a wireless network.

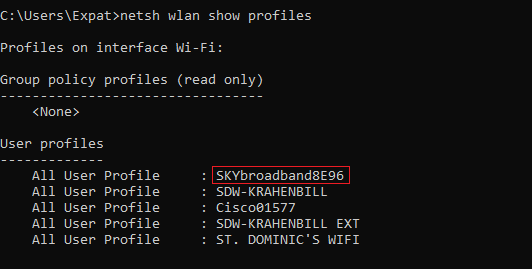
**Overview**

Netsh is a scripting utility provided by Microsoft. It can be used both in command prompt or Windows PowerShell. Netsh is short for network shell. When executed, it provides detailed information about the configuration of the network that the system ever had; including revealing the credentials of wireless networks that it has ever been connected to. This utility comes with various parameters that can be used to get various information as per the requirement. This method can be used both in internal and external penetration testing as netsh commands can be executed both locally and remotely.

To open a command prompt, use your Windows search bar and type, **cmd**.

To get a list of wireless networks your device has been connected to, on your Windows 10 machine open a command prompt and type in the following command:

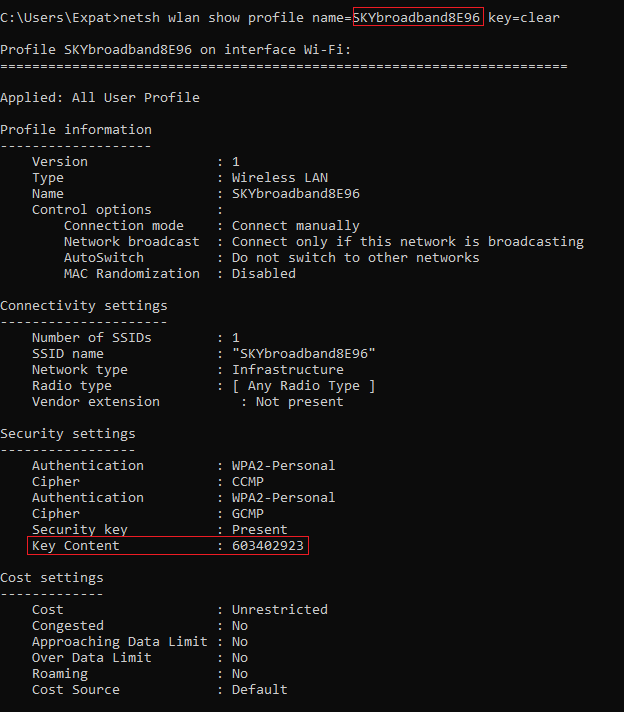
netsh wlan show profiles



Looking at the results from the above command, you can see the names of the Wi-Fi networks that the system has connected to in the past or present such as my **SKYbroadband8E96**. The name has been highlighted in the image above.

To see the password in clear text for my **SKYbroadband8E96** wireless network, I use the following command:

netsh wlan show profile name= SKYbroadband8E96 key=clear



The results of the command can be seen in the output under security settings.

End of the lab!