Lab - Dumping Wi-Fi Credentials Using netsh

Overview

Credential dumping is a technique by which usernames and passwords can be extracted from the target machine. As a pentester or hacker, you may be looking for a way to move around the network laterally.

As a digital forensic investigator, you may want to see what wireless network the suspect's machine has authenticated with in the past. An example would be some type of online cybercriminal activity traced back to a local church. Upon investigation, you discover the church's wireless network has been hacked, and the attacker lives nearby.

You have identified the suspect in the illegal activity. You next need to find proof that the machine did authenticate to the wireless network belonging to the church.

Lab Requirements

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

Overview

Netsh is a Microsoft utility that can be ran using either the command prompt or Windows PowerShell. Netsh is short for network shell. Netsh provides detailed information about the configuration of the network, including the security key for any wireless networks the machine has authenticated with. This method can be used both in internal and external penetration testing as netsh commands can be executed locally and remotely.

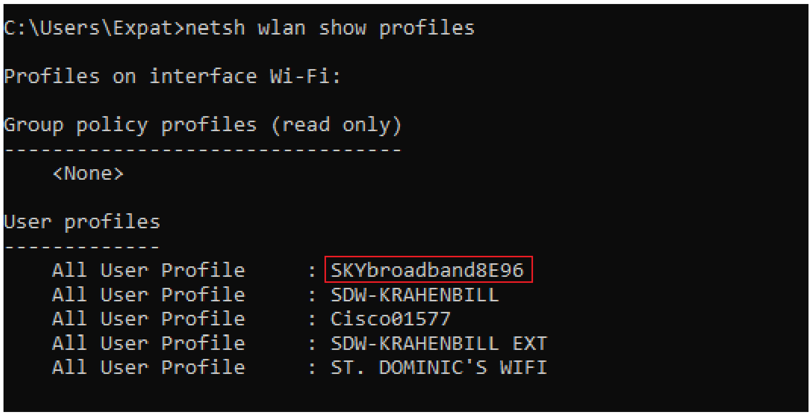
Begin the lab!

On the target machine, open a command prompt or PowerShell and run as administrator.

To open a command prompt, use your Windows search bar and type **`cmd`**. Right-click on the result, and from the context menu, select Run as Administrator.

At the prompt, type in the following command:

```
netsh wlan show profiles
```

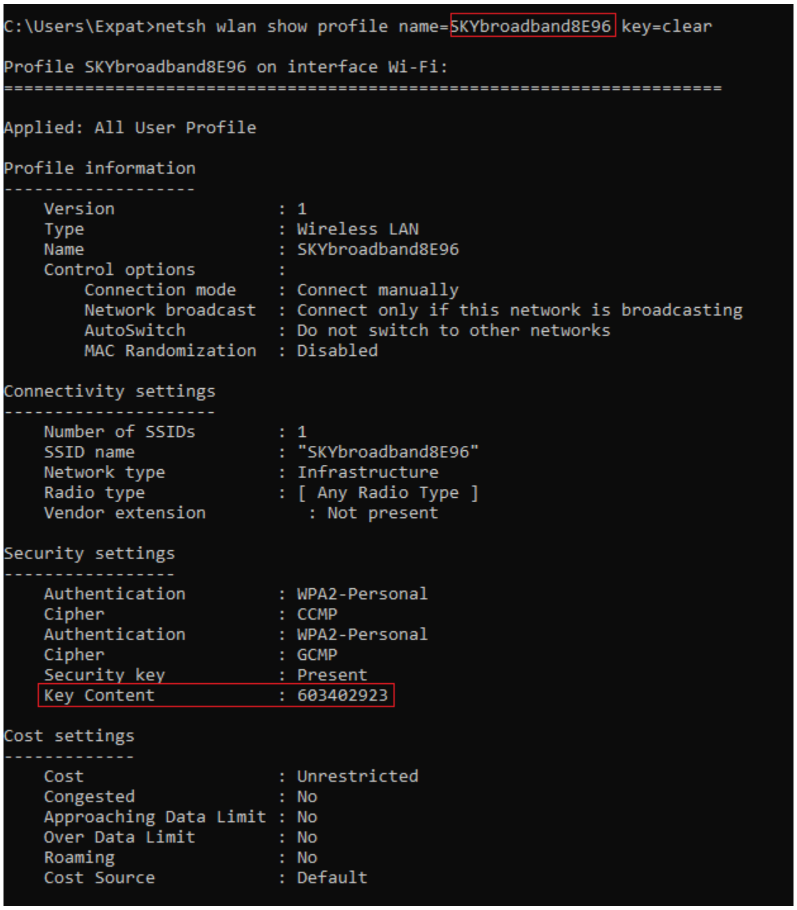


```
C:\Users\Expat>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : SKYbroadband8E96
    All User Profile     : SDW-KRAHENBILL
    All User Profile     : Cisco01577
    All User Profile     : SDW-KRAHENBILL EXT
    All User Profile     : ST. DOMINIC'S WIFI
```

Looking at the results from the above command, you can see the names of the Wi-Fi networks this machine has connected to in the past.

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

```
netsh wlan show profile name= SKYbroadband8E96 key=clear
```



```
C:\Users\Expat>netsh wlan show profile name=SKYbroadband8E96 key=clear

Profile SKYbroadband8E96 on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : SKYbroadband8E96
    Control options        :
        Connection mode    : Connect manually
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "SKYbroadband8E96"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : 603402923

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default
```

The authentication key can be found under Security Settings.

Summary

As a pentester or hacker, you may be looking for a way to move around the network laterally. As a pentester or digital forensics professional, you may need to see what wireless networks a machine has successfully authenticated with in the past. If someone used a wireless network other than their own to perform an illegal activity, their association with that network would be stored as a profile on their machine.

End of the lab!