DNS-Based Phishing Attack in Public Hotspots

By John

101Hacker.com

Abstract— ***this document gives a brief practical insight on how to carry out a DNS-based phishing attack in public Wi-Fi hotspots to trick users into sharing their personal information such as passwords, credit card details etc.***

I. INTRODUCTION

Hotspot:

A hotspot is a site that offers Internet access over a wireless local area network through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi technology.

Hotspots may be found in coffee shops, airports and various other public establishments in many developed urban areas throughout the world

Rogue Access Point /Evil Twin:

Evil twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers

DNS:

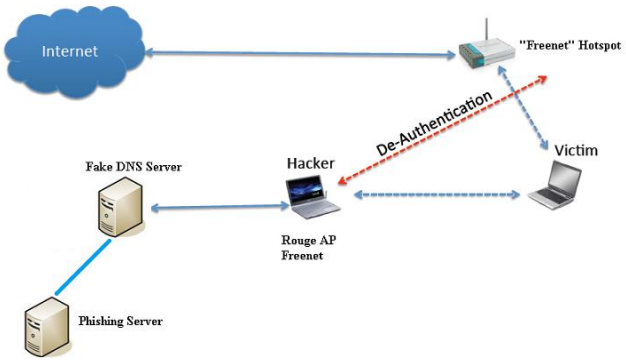
DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers will redirect internet names to different IP address or servers (Fake or phishing servers)

Phishing:

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by appearing as a trustworthy entity in an electronic communication. eBay, PayPal and other online banks are common targets.

DNS- based phishing in hotspots:

In this attack, the attacker initially creates a rogue access point and lures the client to connect to the access point where he runs a fake DNS server. This server redirects particular sites to the attacker's phishing server.



II. PRE-REQUISITES FOR THE ATTACK

The following are the *perquisites* for carrying out the attack

Wireless Card – To create a soft access point, The card must support monitor mode and should be able to inject arbitrary packets in the air .I use alpha AWUSO36H which is compatible with back track OS

Attacker Operating System - Linux with Aircrack-ng suite of tools installed. I use Backtrack which is preinstalled with all the Wi-Fi penetration testing tools

Fake DNS Server: - To redirect websites to our server where we are hosting phishing pages . I use a metasploit auxiliary module "FakeDNS" to setup things easily

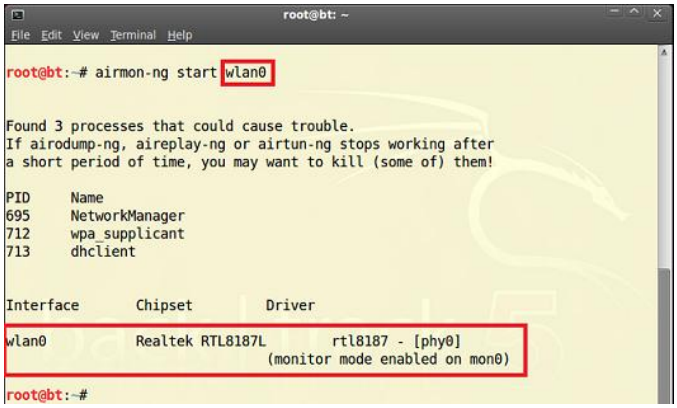
Phishing Server:-
A ordinary server which hosts my fake phishing page and also logs or records all the credentials typed by the victim

III. THE ATTACK

First step is to put the wireless card into monitor mode to monitor the air for finding hotspots in your premise, monitor mode is similar to a promiscuous mode in Lan (local area network). To do this we use a tool called airmon-ng

Command Airmon-ng start (Your wireless interface)

In my case its Airmon-ng start wlan0

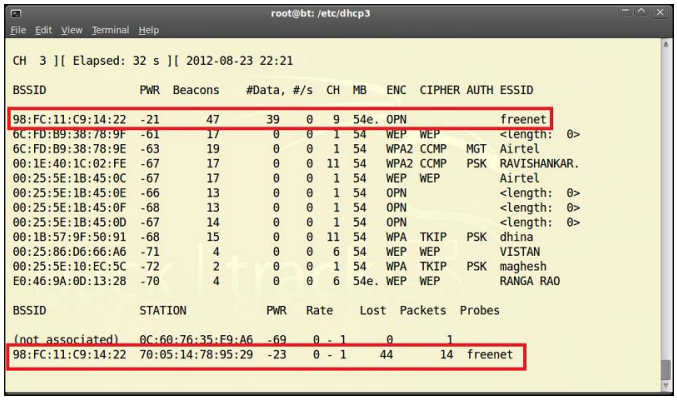


A new monitor interface mon0 will be created as shown in the above picture

Now to monitor the traffic around you we use a tool called airodump-ng

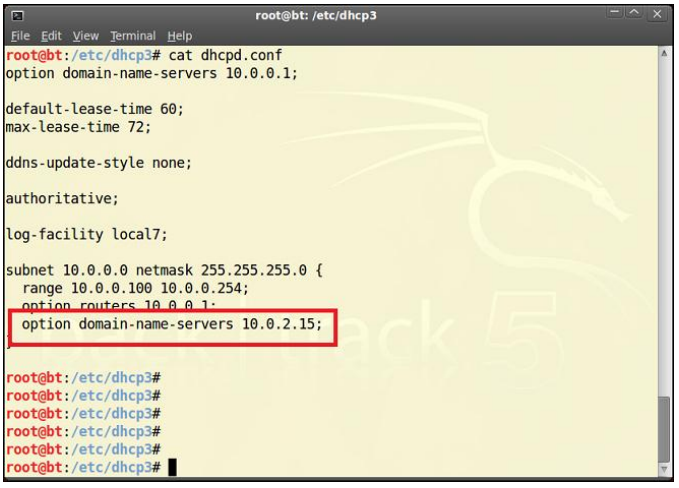
Command Airodump-ng (monitor interface)

In my case its Airodunp-ng mon0



From the above pic I see a hotspot named freenet and I also see a client connected to it

Before proceeding further we configure our dhcp server to enable networking



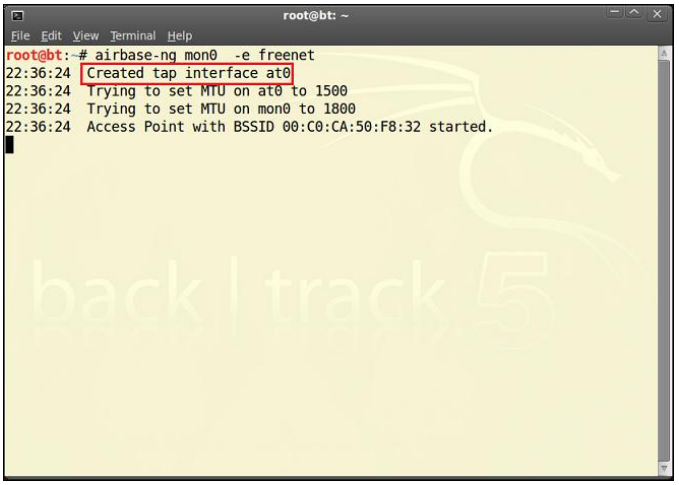
Note :- DNS server is set to my own local ip where i run the Fake Dns Server or Metasploit auxiliary module Fake Dns

Creating Rouge Access Point (Fake Ap) :-

Now we a have to create a fake access point named freenet and make the client connect our Access point instead of the legitimate one

To do this we first create a soft-Ap Using tool called Airbase-ng

airbase-ng -e freenet mon0

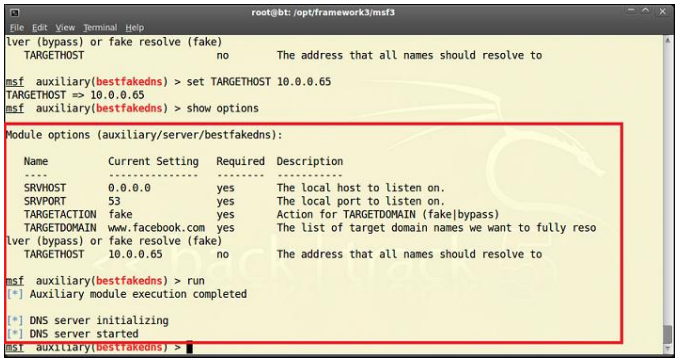


Note: - a tap interface at0 is created as shown in the above picture, we will assign an ip address for it later

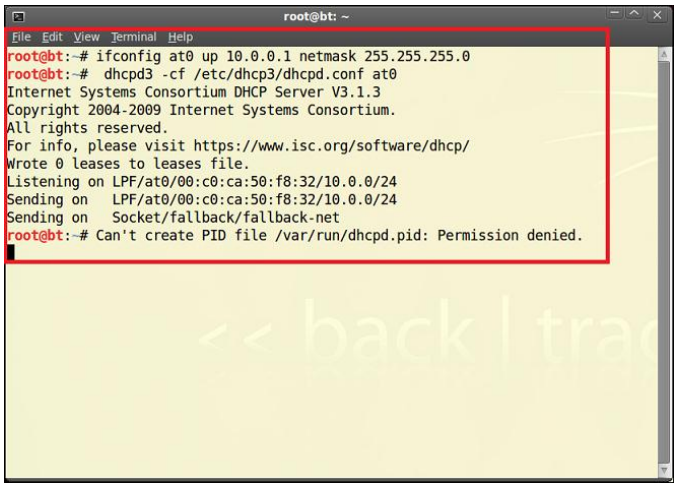
Fake Dns Server:-

I used metasploit auxiliary module FakeDNS to setup my fakeDns server which will redirect the sites set in the

"Target domain" (Facebook is set as an example for our study) to my server where I am hosting my Fake page or Phishing Page



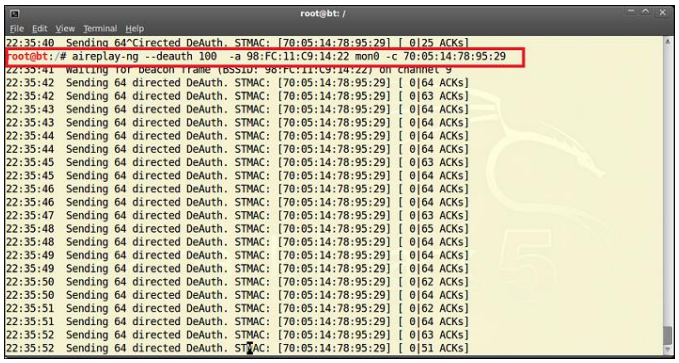
Now we assign an ip address for our tap interface "at0" and bring it up



Making The Client Connect Our Soft-AP(Fake AP):-

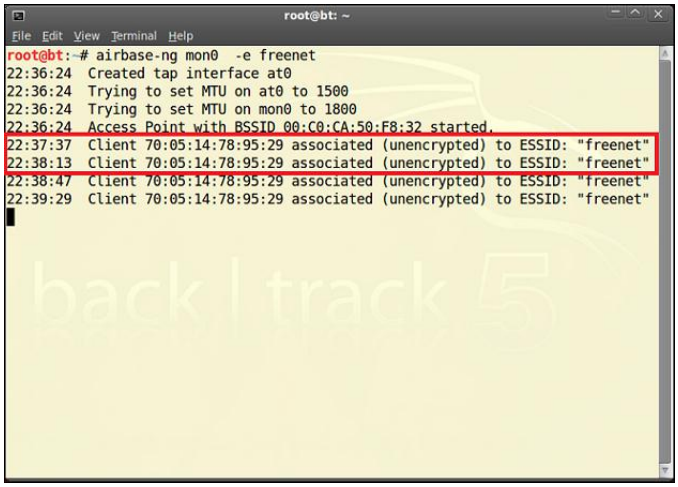
Now we disconnect the client from the legitimate Ap by sending De-auth flood (de-auth packets) to the legitimate AP. We can achieve this by using either aireplay-ng or MDK3

I used aireplay-ng



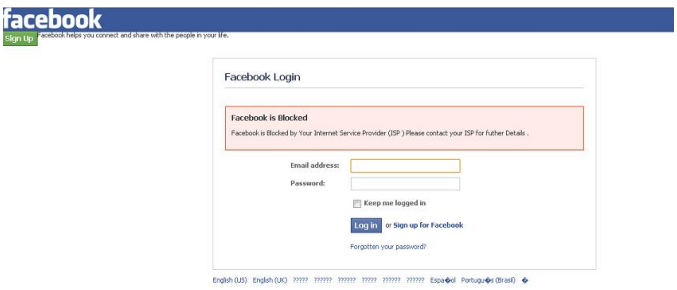
Once this is done the client will be disconnected from the legitimate access point and will connect to my fake access-point without his knowing

We can conform this by looking at the output in airbase-ng tab As shown

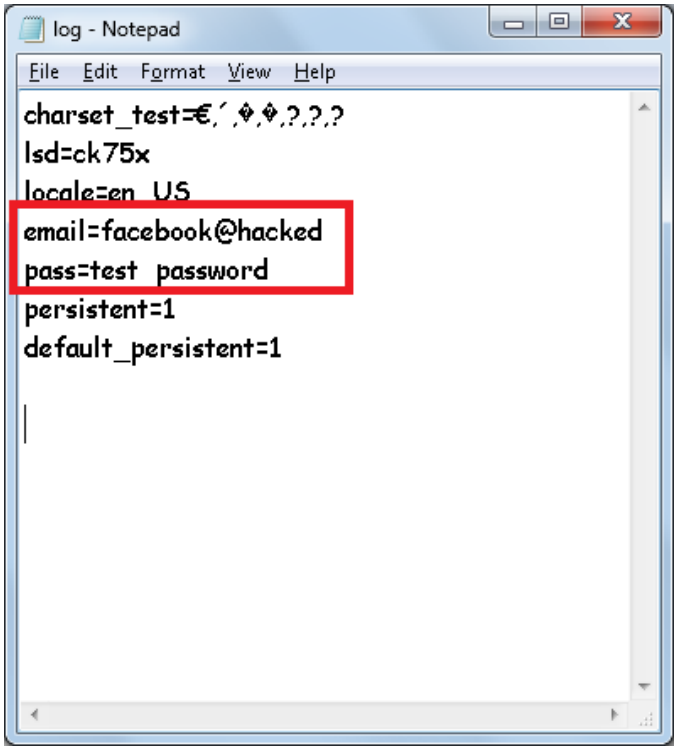


Now whenever the victim tries browse Facebook my fake DNS server will redirect the victim to my phishing server where I host my phisher and rest of the attack is same as in normal phishing attack

The above picture shows the victim viewing my phisher (fake page) which looks like a legitimate one he enters his credentials and tries to login but he is redirected to a different page as destined by the attacker



Meanwhile the victim's credentials are logged (recorded) as shown below.



Thus the victims Facebook credentials are hacked.

The attacker can craft his own phishing page for various social networking sites .Thus this attack is very lethal when carried in a public hotspot such as airports and coffee shops.

IV. COUNTER MEASURES

The following are few counter measures that a user can take to protect themselves from this attack.

i. Always check the sites authenticity
ii. Use VPN when connecting to open hotspots.
iii. When connected to a public hotspot avoid visiting sites that require your credentials.

Note: As on date there are only few counter measures for this kind of attack.

To feel completely secure never use open hotspots.

:

REFERENCES

[1] Wikipedia
[2] Security Tube
[3] 101hacker.com
[4] IEEE
[5] watchguard.com