Wi-fi protected access essay sample

Introduction:

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs. Different WPA versions and protection mechanisms can be distinguished based on the (chronological) version of WPA, the target end-user (according to the method of authentication key distribution), and the encryption protocol used. There are many attacks to hack WPA/WPA2, in the environment of LINUX system (Using the Backtrack) we can find a lot of tools in Backteack5 and the most famous methods in backtrack are REAVER and Dictionary attacks. The second way use a dictionary file or world list that contain vary large amount of possible passwords to test it but if the password not stored on the file it will not be cracked , on the other hand the REAVER method more able to crack WPA/WPA2

2-About REAVER method:

REAVER … it is an open source tool that brute forces WPA/WPA2 and exploits a security hole in wireless routers and can crack most routers. It’s tied to a PIN that’s hard-coded into the device. Reaver exploits a flaw in these PINs; the result is that, with enough time, it can reveal your WPA or WPA2 password.

* 3-How to protect yourself against Reaver attacks:

* Your network should be safe if you can simply turn off WPS (or, even better, if your router doesn’t support it in the first place). Even with WPS manually turned off through his router’s settings, Reaver was still able to crack his password but it reduces the possibility. * You could also set up MAC address filtering on your router (which only allows specifically white listed devices to

connect to your network), but a sufficiently savvy hacker could detect the MAC address of a white listed device and use MAC address spoofing to imitate that computer. * SO if the open-source router firmware DD-WRT installed on the router, can unable to use Reaver to crack its password. As it turns out, DD-WRT does not support WPS It’s a good security upgrade, and DD-WRT can also do cool things like monitor your internet usage, set up a network hard drive, act as a whole-house ad blocker, boost the range of your Wi-Fi network.

4-example of REAVER attack:
First, if the REAVER not installed on your backtrack you must DOWNLOAD it….. Click the Terminal button in the menu bar (or click Applications > Accessories > Terminal). At the prompt, type: apt-get update

And then, after the update completes: apt-get install Reaver

Then you must to find your wireless card using airmon-ng , so write ; airmon-ng

Then you must to put your wireless card into monitor mode: airmon-ng start wlan0

Then you must to Find the BSSID(MAC) of the router you want to crack using airodump-ng on monitoring interface you have, so write; airodump-ng mon0

Then when you chose your target, copy the BSSID to do the Reaver on it, and it takes arguments –i[your interface] and -b [BSSID] –vv[vector, vector]; reaver -i mon0 -b 8D: AE: 9D: 65: 1F: B2 -vv