

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to DOS Wireless Access Points! Wireless Chaos #2](#)

IbnuAbee - February 6, 2014, 3:30 am

Hi guys,

This is my second tutorial on wireless chaos. I can't seem to find too on this field here, so I thought I could help out with that. This tutorial will go through teaching you how to DOS a wireless AP.

We'll be using MDK3 for this tutorial and specifically the Intelligent Authentication Mode that comes in the suite.

So, let's get started.

But before beginning, ensure you have monitor mode switched on.

If you plan on targeting a specific AP, you would need to type the following into terminal to get the MAC address of the targeted AP.

Quote:"iwlist wlan0 scan"

Alright, so what you want to do, is open up Applications > Backtrack > Stress Testing > Wireless Stress Testing > MDK3.

It's quite simple, when targeting a specific AP, type in the following

Quote:"./mdk3 a -a <AP'sMAC>"

If, however, you want MDK3 to attempt the attack on all the routers it can reach, type in the following instead.

Quote:"./mdk3 a"

Do not worry about it saying that the AP seems invulnerable, it'll say that until it goes down.

[img]http://i94.photobucket.com/albums/l112/TAPE_RULEZ/mdk3-authdos.jpg[/img]

And give it a while, as some routers may take up to ten minutes (I've seen many go down in the first minute). To boost the speed, attempt with 2 laptops, and it should be a whole lot faster.

This attack works almost all the time however some routers have an anti-DOS protection system implemented blocking such attacks.

Hope you liked my tutorial, please do leave feedback below. Enjoy! ?

IJigsawI - February 6, 2014, 3:51 am

Nice tut OP. Will give this a try sometime :)

TheHackingMonkey - February 6, 2014, 3:55 am

Good tut OP. Will try this one day for sure. :D

IbnuAbee - February 6, 2014, 3:56 am

Thanks, this hack could be used in combination with, say, a fake AP, which would make the chances of getting a password a lot higher and reduce the level of suspicion as there would only be one AP with the target AP's name.

CtrlAltDelete - February 9, 2015, 3:10 am

Quick Question: Kali running on VMWare doesn't seem to have a wireless interface. eth0 doesn't work for me, do I have to boot it on a physical machine?

ExclenKr - February 9, 2015, 11:14 am

Well how can I run my exe silently over lan? i don't want to go with dns spoofing, fake update etc.

dadada12 - February 22, 2015, 5:18 am

Thanks man, now i know what to do, Great tutorial :)

YssDiamond - June 21, 2016, 12:31 pm

Nice Man Great Tutorial 10/10