

Forum: [Hack Forums](#)

Thread: [\(just a thought\) -finding a new wpa exploit.](#)

HackRain - May 6, 2011, 1:05 pm

Hey guys.

i was laying in bed last night cracking wpa. sitting.. waiting..
as you all know it can be time conserving waiting for pyrit/aircrack to do its thing.

i started thinking about how aircrack de-authenticates the slave of the router.
if im correct, aircrack sends a protocol to the router, that asks it to deauth the user. or "forcefully"
tells it to correct?

i was thinking, do you guys think its possible to send a protocol and/or send a lot of protocols in
which may "dos" or "flood" the router, so it reset's.

i realise that re-setting the router wont hard reset it but nearly re-boot it. but then i was thinking, if
there i a client, he will have to re-connect to the router, is it possible to set up a sniffer in between
him and the router. so as he logs on, we get the un-encrypted password?
or something like that?

i know that seems far fetched. but im hoping to start a little thinking group here, and see what
people come up with.

=]

Middle - May 6, 2011, 1:20 pm

You could use airdrop-ng to deauth the clients then when they rejoin you capture the handshake,
but that is exactly the same as before...

HackRain - May 6, 2011, 1:28 pm

hmm,

yes but without the router, there is no encryption over the key.

when u kick a client, he has to connect to the router and it gets encrypted, if u kick the router first,
the user holds the key and then the router has to et back up and then recive the key.
oh wate..

man i think your right.. its exactly the same isnt it middle. well not much different.

well is it possibel to do this!

change

ser up a router, or a fake ap, and change the essid to clone the slaves essid. then kick the client
and reset the router, since the client connects automaticaly, we get connected to and therfore the
password ?

how about you middle, u have any ideas

CXDBrightSide - May 6, 2011, 2:29 pm

(May 6, 2011 01:28 PM)PandaMonix Wrote: [\[CITE\]](#) hmm,
yes but without the router, there is no encryption over the key.

when u kick a client, he has to connect to the router and it gets encrypted, if u kick the router first, the user holds the key and then the router has to get back up and then receive the key.
oh wate..

man i think your right.. its exactly the same isnt it middle. well not much different.

well is it possible to do this!

change

set up a router, or a fake ap, and change the ssid to clone the slaves ssid. then kick the client and reset the router, since the client connects automatically, we get connected to and therefore the password ?

how about you middle, u have any ideas

I think you may be on to something with the fake ssid. But wouldn't you need to fake the ssid/bssid? I don't know how all wireless cards work but I know that neither my laptop or iPod touch will auto-connect without both being identical. And once they send the pass, what would you use to capture it (I can think of a few options, just not sure what the best would be) and would it show the pass in plain text or would it still be encrypted, since it's encrypted before it's sent? It sounds like unless you already had the pass set for the fake AP it would just reject their pass...but I don't know, I'm still pretty new to this...

HackRain - May 6, 2011, 2:34 pm

it would not be encrypted.. or if it were, it would be encrypted in my chosen encryption. it is my access point. i could run something like cain and abel.. to get the password.

either way getting the password is the easier part. its trying to fake an access point and get someone to connect. thats my worry.

M A T R I X - May 6, 2011, 2:37 pm

Even if you rebooted the router, it wouldnt set it default. If thats your objective. If not sorry.. You have to do a 30.30.30 (hardboot)

HackRain - May 6, 2011, 2:46 pm

matrix - im not looking to hard boot it. all im trying to do is get it to reset. while it boots up, i want to fake an ap that is a clone.

that way he will connect to my ap and give me the key.

CXDBrightSide - May 6, 2011, 2:49 pm

It sounds plausible, though I've never heard of it being implemented.

HackRain - May 6, 2011, 2:53 pm

exactly. thats why i said a new exploit thought =]

if i can get this working.. then there going to have to release a new security wpa3 lol. because if u think about it, this technique (if it workes) is a 100% hack. like wep

CXDBrightSide - May 6, 2011, 3:03 pm

That is, if everyone in the world can make a fake AP. I don't know the command to specify a custom/spoofed BSSID so I'm not much use -.-

HackRain - May 6, 2011, 3:12 pm

haha iv been thinking about that and i first thought

i could change my essid of my router, then find a way to spoof the mac of it... but i think thats impossible.

then i realised im running an intel n6300 and it supports intels wifi technology. meaning i can make a custom access point with my laptop. even further more.. i can spood my mac address becus it takes the bssid from my wifi card.

so i can spoof my mac vie the macchanger. then creat an essid thats a clone with intels wifi technology.

i think that could work. the only problem is, my "wifi technologyu is on windows side only =/"

CXDBrightSide - May 6, 2011, 3:14 pm

Ooh...Windows. That could be a problem. Maybe run VMWare after getting your spoofed AP running? I don't know if the traffic on the card would interfere with BackTrack sending the deauth, but I doubt it'd work. You might have to do with with two wifi cards.

HackRain - May 6, 2011, 3:18 pm

im going to search for a windows alternative macchanger if possible. btw i dont use backtrack i use ubuntu 10.10 XD

CXDBrightSide - May 6, 2011, 3:21 pm

Ah, either way, I meant to type aireplay-ng in the first place but my mind went blank for a second.

HackRain - May 6, 2011, 3:23 pm

ok, well i think it can be done with 2 computers a lot simpler. one doing an attack, anouther being an access point.

but id like to work it out with 1 computer.

anyone up for trying it with me.

Middle - May 6, 2011, 3:53 pm

Well if you are looking for alternative methods i can come up with a couple:

1) Go and SE your way into the building and then use WirelessKeyView on a PC or get access to the router and look for default settings on the back and hard reset

2) *You will like this one*, Clone the WPA AP, then use airdrop-ng to disconnect all the users from target AP, and boot them on to yours (Its cloned), then DNS spoof the users to a page saying 'Router error: Please re-enter your wireless key and router password', phish the input from their and then allow your own MAC to connect to the target AP using airdrop-ng + the wireless key (but still denying the others access) then you have access to the network + the router. Once you have had a look at the router settings, get the clients back on the network by killing airdrop-ng and your fake AP.

Never done it myself, but perhaps if you got really dedicated you could get that to work. However i still maintain the easiest way is to use social engineering, like is explained in my tutorials.

CXDBrightSide - May 6, 2011, 9:50 pm

The DNS spoofing sounds MUCH easier than what you were talking about with Cain and Abel, if that would even work. That's pretty much the only question I had unanswered, gonna try this out when I'm actually around other people using WPA.

HackRain - May 7, 2011, 2:01 am

(May 6, 2011 03:53 PM)~Middle Wrote: [\[CITE\]](#) Well if you are looking for alternative methods i can come up with a couple:

1) Go and SE your way into the building and then use WirelessKeyView on a PC or get access to the router and look for default settings on the back and hard reset

2) *You will like this one*, Clone the WPA AP, then use airdrop-ng to disconnect all the users from target AP, and boot them on to yours (Its cloned), then DNS spoof the users to a page saying 'Router error: Please re-enter your wireless key and router password', phish the input from their and then allow your own MAC to connect to the target AP using airdrop-ng + the wireless key (but still denying the others access) then you have access to the network + the router. Once you have had a look at the router settings, get the clients back on the network by killing airdrop-ng and your fake AP.

Never done it myself, but perhaps if you got really dedicated you could get that to work. However i still maintain the easiest way is to use social engineering, like is explained in my tutorials.
the second one is exactly what iv been trying to do.

i didnt even know it was possible to creat a phish over wireless.

CXDBrightSide - May 7, 2011, 10:16 am

Through [DNS spoofing](#) it is.