

Forum:[Hack Forums](#)

Thread: [Getting a serial number of an Actiontec router remotely](#)

ownercj - January 18, 2014, 12:41 pm

I want to portforward my neighbors router for my rat since I cannot use my router. I used this program from here:

<https://hackforums.net/archive/index.php/thread-1500197.html>

and it gave me the serial number of one of my neighbor's routers. I have access to three of my neighbor's access points but they're so far away that it's impractical to use for anything. The two that are farthest away (obviously) are the only ones that have the default username and password for the router login. The one that is closest however; has a different password, I've tried all the default passwords and none of them worked. I know that the router they use is an Actiontec (commonly used and sold by Verizon and Frontier). I read online that in order to improve security, Verizon updated the password to the serial number of the router. The program I used for the upnp port forwarding gave me the serial number of one of the farther routers and I thought: "Wonderful, now I can use it on this one and I can get the password." Obviously, it's not that easy... The program doesn't succeed in getting the serial number and in fact, it doesn't even detect anything about the current access point I was on (no default gateway, router model, ISP... nothing). I don't know why or how this program manages to get the serial number for one router and it doesn't for another one. I'm positive that all the routers are manufactured by Actiontec, as that is what Frontier communications provides as the packaged router when you purchase Internet from them. But, the reason why I'm so sure that my neighbors haven't changed their router (95% sure) is because they use WEP security and that is what was probably standard encryption back when they purchased the router.

Is there any way that I could get the serial number (other than walking over to my neighbor's house and asking or looking for it --I know that much.) I heard of using the Miranda python script in Backtrack 5r3 to use a upnp exploit to permanently forward a port; however it was ineffective against this router. If there is any information that I could add to this that could help you help me, I'll get it for you. Any help would be greatly appreciated.

Joseph Ducreux - January 18, 2014, 5:55 pm

use airodump-ng to obtain the exact model and mac address to use OUI to get default admin/username router info, otherwise use hydra to bruteforce this, use WPS to obtain the serial

ownercj - January 19, 2014, 9:35 am

(Jan 18, 2014 06:55 PM)CEAZE Wrote: [\[CITE\]](#) use airodump-ng to obtain the exact model and mac address to use OUI to get default admin/username router info, otherwise use hydra to bruteforce this, use WPS to obtain the serial I tried using this command :

<https://i.imgur.com/a0Xlj8P.png>

but airodump didn't find the router manufacturer or model. Is there anything that I missed? I think I must be doing something wrong because the other AP I already have the serial number for (Essid: RBP6L) also doesn't show the manufacturer. But on Windows when I ran the port forwarding tool, it gave me all sorts of information on RBP6L. I don't think hydra will be useful bruteforcing this router because this router ciphers the text you enter into the password field (like if I type in the letter 'a' it will show three hidden characters in the password field). However, if they did change it and I'm wrong about the password for the router control panel being the serial number of the router... I did find this python script someone made specifically for the different login page you get when you visit the router login page here (this is why I'm pretty sure that this router is an Actiontec router, but I still don't know the model number):

<https://code.google.com/p/joelisester-sandbox/downloads/detail?name=crackvfrouter.py&can=2&q=>

I guess at this point anything is at least worth a shot doing, but if the password of the router is the serial number-- then brute forcing with hydra will most likely fail (unless the serial number happens to be 111111).

Also, I'm not quite sure what OUI is or how I can use it to gain the password, nor what script I should use to use WPS to get the serial number. I know reaver is a good script to use if you want to get the WPS pin to get access to the wifi on the access point; however, I already have access to the wifi provided on the AP, unless you're thinking that the pin could be useful somewhere else (I'm still a noob, sorry). Do you have any other ideas of what I can do? Thanks for your help so far, I appreciate it a lot.

I don't know why I haven't found this before... I fell like a complete idiot because I haven't found this.

<https://i.imgur.com/nnQrNob.png>

I tested the serial number in the router login page (obviously...), it didn't work. So whoever owned the router must have been smart enough to make their own password. I Googled and I found this spreadsheet:

http://support.actiontec.com/doc_files/Current_Firmware_Versions.pdf

their ISP is Frontier, so the model number is either: MI424WRE or MI424WRF. I'll look for exploits for these model numbers; but, does any of that information help get me any further by means of a wireless attack?