

Free WiFi in Airports & Public Hotspots

By,

Brian Wilson

CCNA, CSE, CCAI, MCP, Network+

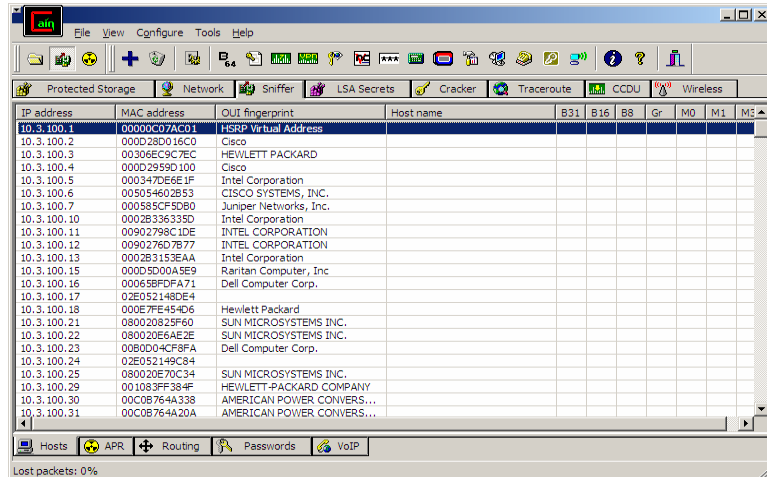
Slimjim100@slimjim100.com

www.middlegeorgia.org

www.slimjim100.com

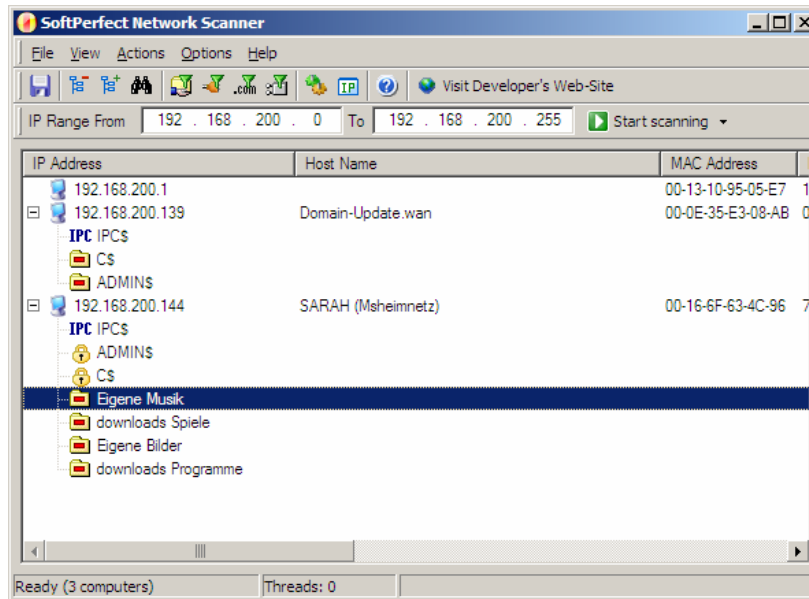
Disclaimer: This paper and the topics covered in the paper are just for educational purposes and should not be used on a network without permission from owner of the network you plan on testing. I hold no respectability for any actions or damage that might accrue if you try anything explained in this paper. "do not do this at home kids" hacking/cracking/pen testing might be harmful to your health.

Recently while traveling I noticed a hot spot and wanted to surf the internet. Once I connected to the AP I had seen that they wanted to charge me \$8 per day to surf the internet. I thought that was just too much money for a quick internet connection and my layover between flights was about 3 hours. I decided to see what I could access while connected to there AP. Well I got to there splash screen and it would allow me to surf on that page and the local ISP's home page (the local ISP was there sponsor). Any other sites would not work and force my browser back to the splash screen trying to get me to pay them the eight dollars to surf. With my experience in setting up content portals on AP's I noticed this portal acted a lot like Monowall (www.mon0.ch). Since I know how the security features in Monowall worked (using MAC addresses to block content) I wondered if I could get past the portals firewall with out paying the service fee. I wanted to do this just to see if it could be done and to gage the security of this network. Well first thing I did was scan the subnet I was on to see what I could access. For the scanning software I used Cain & Able (www.oxid.it) and I also used SoftPerfect's Network Scanner (www.softperfect.com). The reason I used Cain & able was because it provided an easy to use interface and I wanted to see if the hosts on the subnet with me where visible and if they could be pinged.



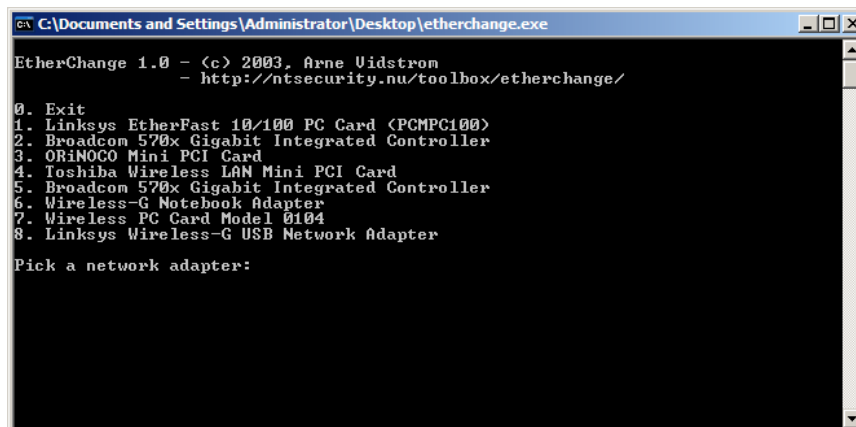
IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
10.3.100.1	0000C07AC01	HSPR Virtual Address								
10.3.100.2	000D28D016C0	Cisco								
10.3.100.3	00306EC9C7EC	HEWLETT PACKARD								
10.3.100.4	000D2959D100	Cisco								
10.3.100.5	000347D6E61F	Intel Corporation								
10.3.100.6	005054602B53	CISCO SYSTEMS, INC.								
10.3.100.7	000585CF5DB0	Juniper Networks, Inc.								
10.3.100.10	0002B336335D	Intel Corporation								
10.3.100.11	00902798C1DE	INTEL CORPORATION								
10.3.100.12	0090276D7B77	INTEL CORPORATION								
10.3.100.13	0002B3153EAA	Intel Corporation								
10.3.100.15	000D5D00A5E9	Raritan Computer, Inc								
10.3.100.16	00065BDFFA71	Dell Computer Corp.								
10.3.100.17	02E052148DE4									
10.3.100.18	000E7FE454D6	Hewlett Packard								
10.3.100.21	080020825F60	SUN MICROSYSTEMS INC.								
10.3.100.22	080020E6AE2E	SUN MICROSYSTEMS INC.								
10.3.100.23	0080D04CF8FA	Dell Computer Corp.								
10.3.100.24	02E052149C84									
10.3.100.25	080020E70C34	SUN MICROSYSTEMS INC.								
10.3.100.29	001063FF384F	HEWLETT-PACKARD COMPANY								
10.3.100.30	00C0B764A338	AMERICAN POWER CONVERS...								
10.3.100.31	00C0B764A20A	AMERICAN POWER CONVERS...								

Cain & Able Sniffers menu.



SoftPerfect Network Scanner

Once I received the results of the scanned subnet and seen all the other computers along side of me. I noted the content filter/firewall claimed all the unused IPs but I was able to see the difference from the firewalls MAC and the other PC's MAC. I then tried a ping test and I got responses to my pings. I was able to verify the hosts where active and with a little sniffing I seen who was pulling traffic outside of the firewalls restrictions. So thus far I have found that the firewall was not letting me out of the network freely but I was able to play inside of the LAN subnet with out interaction. I am able to scan and sniff the local subnet and the firewall is not blocking me from thoer host on the subnet. Now it is time to see if spoofing my MAC address with another paid PC would let me out to surf. I used EtherChange (www.ntsecurity.nu/toolbox) to clone my MAC address to match one of the other PC's I noticed pulling lots of traffic.



EtherChange by www.NTSecurity.NU

Low and behold this was the key to getting past the content filter firewall and I am able to surf the internet without the firewalls blocks. I now checked with my sniffer to make sure I did not stop the internet connection form the nice PC that loaned me it's

MAC address. Good news was that the firewall let us both surf the internet with different IP's and the same MAC address. I conclude that this content filter was only blocking users by MAC address and once you paid the fee and had your MAC address added to it white list any PC with that MAC was also free to surf the internet. This kind of MAC security is the same many home AP's use to mis-inform customer that they are secure. I see this as a real flaw and it is not a real security feature as anyone that has basic skills can get around it. With this being the security on that network I only hope the Airport uses better security on there internal network. I am now ready to test the next AP that blocks my internet to see how it implements security. Please note I did pay for service after testing the AP and I was not cracking anything. If anyone else happen to have the same MAC as a user that paid in the last 24 hours this would have happened anyway. Some day soon people will understand the need of real network security and the internet will be a safer place. Remember that tricking a paid service for free service is stealing and there are consequences to that so be ready to pay the price if you get caught stealing. I do not recommend trying anything here I have explained without permission from the owner of that network.