

Cain & Able  
**Brian Wilson**  
CCNA, CSE, CCAI, MCP, Network+  
[Slimjim100@gmail.com](mailto:slimjim100@gmail.com)  
[www.middlegeorgia.org](http://www.middlegeorgia.org)  
[www.middlegeorgia.info](http://www.middlegeorgia.info)  
(AKA Slimjim100)

Ok I will start this article out with the place to find and download Cain & Able software ([www.oxid.it](http://www.oxid.it)). What is it you may ask? Well its like a Leatherman WAVE for your LAN. Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing and scanning the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks (Rainbow Tables), decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. This software also lets you spoof your IP & MAC to make life hell for any admin trying to find you on the subnet, but I don't recommend tiring this unless you have permission to do so. Other fun stuff Cain offers WiFi scanning, Cisco config downloading (via SNMP), support for pocket PC, and a lot of fun with NetBIOS scanning domains.

Version 2.8.9 is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time. VoIP Recording for logging all you nice Voice over IP calls. The sniffer can also analyze encrypted protocols such as SSH-1 and HTTPS if used with APR and a Man-in-the-middle situation. You are also able to Man-In-the-Middle RDP sessions to get key logs. Other cool tools are the DNS spoofing that will allow you to spoof DNS request (if a client on the subnet is trying to get to Google you can send them to yahoo). Cain also sniffs routing protocols, https Certs, monitors and routes packets, crackers for all common hashing algorithms and for other various specific authentications, password calculators. Other tools are Sid-Scanner, LSA Secrets Dumper, Protected Storage Passwords Viewer, NT Hash-Dumper. Now for the Abel remote service features and uses. With Able installed on a remote PC you can use Remote Console (command line), Remote Hash dumper, Service scanner, Routes, and many other useful tools. So now you are wondering what all this means. Well with free software that offers all of these utilities in one application it can be a life saver if you lost a password on a system or if you're a freelance consultant that has to fix poorly maintained networks. As always I do not endorse any mis-use of software but I do endorse learning on a safe network in the effort that it will help you to secure your own network. Some of the most useful features I use Cain for are Active Directory scanning, Password sniffing, remote drive mapping, remote hash dumping, Password Cracking (Dictionary, Burteforce, Rainbow Tables), Network sniffing, DNS Spoofing, Wireless Scanning, and just keeping an eye on your network. I have only covered some of the features Cain has to offer you. I recommend reading the help file included with the software as it is an awesome resource for all things Cain. If you have any question regarding how to use Cain or tweak it just e-mail me [slimjim100@gmail.com](mailto:slimjim100@gmail.com).



