1. Research and post information concerning tools that are used for identifying Vulnerabilities on systems. Must include the following:
   1. Be specific on what features the tool has.
   2. Compare at least two specific tools that you may or may not have used.
   3. Backup your assessment with concrete references to others who have either worked with the tools you are addressing or have researched the tools before you.
2. There is a separate assignment associated with this week's topic. [Check out the assignment.](https://suu.instructure.com/courses/355040/assignments/2587926)

I decided to do some more research on brute force password cracking tools. Brute Force is a term used to describe a trial and error method used to decode passwords, and keys. Essentially brute force cracking is going through and trying every possible combination characters to figure out a pass phrase. It is like a thief trying every possible combination on a safe inorder to discover the combination. This is a very time consuming process, but very effective. A way to prevent Brute Force is locking account. Locking accounts is the process of simply locking an account after a certain number of failed password attempts. What I discovered alot of password cracking software/tools out there. I have used several without really thinking about it, like cain and abel, john the ripper, ophcrack, and Forensics Toolkit (FTK). Cain and Abel and John the Ripper are what I’m going to talk about.

Cain and Abel: Probably the most widely known password cracking tool. Cain and Abel can work as a network sniffer, cracking encrypted passwords, open source, recording VoIP, finding cached passwords, analyzing routing protocols, WEP cracking, ARP Spoofing, IP to MAC address recovery, and ofcourse brute force attack. Some of the downsides to C&A is only a Windows only software, Rainbow tables must be downloaded, administrator access, hard to use other built in hacking tools, and currently doesnt run on all windows OS’s. C&A is fast and free but depending on what you are trying to get into this tool might not be the best option.

John the Ripper: another well known password cracking tool. John the Ripper is a open source tool for linux, unix, windows, and MAC OS’s. I personally have only used this on linux. With john the ripper is very popular, combines a number of password crackers into one package, autodetects password hash types, customizable cracker, can be run against different password formats, and is opensource. This tool doesnt have any of the network capabilities that Cain and Abel have.

Honestly it is depending on what you are trying to do. I believe that John the ripper is a better password cracker, but I have used Cain and Abel to do so WEP cracking and password cracking they both work fine.

<https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks>

<http://blog.windowsloginrecovery.com/pros-and-cons-of-cain-abe-windows-password-recovery-tool.html>

<http://www.oxid.it/ca_um/>

<http://www.openwall.com/john/>

<https://neverendingsecurity.wordpress.com/tag/john-the-ripper/>

<http://resources.infosecinstitute.com/10-popular-password-cracking-tools/>