Elcomsoft Wireless Security Auditor in regulatory and audit situations

By Daniel H., IT Security Analyst

In this era of increasing audit compliance – whether it's PCI, HIPAA, SOX, NERC/CIP, PCI or even Internal Audit, having the evidence to prove your organization is compliant and secure is a major undertaking. Frequently, organizations worldwide have not just one, but multiple regulatory requirements to deal with. As regulations mature, the risk of increased penalties and fines that can be imposed on an organization also grows, making compliancy a major issue. One favorite technical target for external and internal auditors is wireless networks. With the massive proliferation of wireless networks, modern organizations need a way to prove their wireless networks are reasonably secure without divulging their network passphrases or keys to the auditing party. How can a company or entity prove it is worthy of a passing grade when they are using a technology that is widely known to be a major source of vulnerability?

Welcome Elcomsoft's Wireless Security Auditor (EWSA). At first glance, you may think of Elcomsoft's Wireless Security Auditor (EWSA) as only a tool that gives hackers or penetration testers way to crack network keys, and thus invariably prove you're network security is LACKING instead of the other way around. It's true, Elcomsoft's Wireless Security Auditor is capable of blasting through some "secure" networks with ease, and not just simple dictionary or commonly used passwords. In fact, the tool is capable of some pretty amazing feats – EWSA runs primarily on Windows™ platform and utilizes graphics cards such as nVidia or ATI to parse large amounts of data in a small amount of time, giving a major boost in cracking times. For example, a WPA2 password that once took months or years to crack can now be cracked on your nearest gaming PC (One that could very well be in your living room) in less than a few hours.

Take our machine for example: Running a respectable Intel i7-860 processor and an nVidia GeForce GTX 480 graphics card – I was able to crack our lab's wireless network in less than 5 hours. EWSA was able to run through an average of 23,000 passwords per second, 400 million passwords in 5 hours.

Right now you might be asking yourself – how does this help me with compliance at all? The answer comes from a surprising source – a growing number of industry standard auditors. Using a sort-of reversed sense of logic, similar to non-repudiation, you can prove that someone using a tool such as EWSA would NOT be able to compromise your network in any reasonable scenario. Auditors love evidence. If you can hand them a report, generated from the unsuccessful attempt of Elcomsoft's Wireless Security Auditor, you're a step closer to proving compliancy in their eyes. Now, obviously not all auditors come from the same school of thought, but in the absence of some other types of evidence, this audit logic and subsequent evidence generated with EWSA might be the deciding factor on whether the audit team needs to "dig further" or can move on to other areas.

Some technical tips on generating reasonable evidence with Elcomsoft's Wireless Security Auditor:

- Make sure your wireless network is actually using a secure passwords or shared keys! Adding a few special characters or upper case letters to a word or two will not make a password secure. With EWSA's ability to "mutate" dictionaries, a password like '$securewireless$' can easily be exposed. A password at least 16 characters in length with "random" upper, lower, special, numbers will be the most effective countermeasure.
- Use a large dictionary file. The larger the dictionary file, the better the password audit will look in the eyes of an auditor. There's no specific right or wrong size, but if you use a dictionary with 200 words, expect the password audit to fail the "laugh test". Use, at the very least, the password dictionary that comes with Elcomsoft's Wireless Security Auditor.
- Max out the mutation settings in the Advanced section. This will prove that you went above and beyond the call of duty and made every reasonable attempt to crack your own network with EWSA.
- Make sure you document your methodology. Obviously, only using EWSA to provide evidence for an audit will not suffice, however it is valuable evidence and needs to be documented properly. Make sure to document the thought process behind this piece of evidence, or it may be interpreted wrong by some auditors.
- Use the "Laugh Test" yourself. If you find yourself laughing under your breath at the thought of using something like this to provide evidence for your audit, it may not be right for you. No regulation is built the same and the same goes for audit teams. An internal auditor may be much harder on you than a federal regulation committee or audit team. Even 3rd party auditors for audits like NERC/CIP may differ from one to the next. Use caution, and have mitigating factors that can provide the much needed "Get out of jail free card".

All of these audit points aside, Elcomsoft's tool is still extremely valuable even if it is not run in this capacity. Verifying your company's wireless networks may reveal a nasty truth about your organization's insecurities, or more preferably, verify your security is at the level it can best achieve. In password cracking, looking past the hardware perspective, beyond limitations and commonly known obstacles, unique tools such as Elcomsoft's Wireless Security Auditor take information security and protection to a new level.