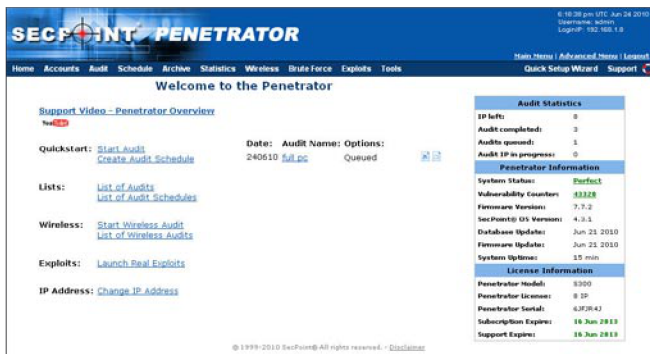


Secpoint Penetrator

by Michael Munt

The Secpoint Penetrator S300 comes in a small form factor Dell Optiplex unit. All you need to do is plug it in as the operating system and programs etc are already pre-configured for ease of use. Just connect to the system via your local machines' browser and you're ready to go. Once you are logged in you are presented with the following screen;



Auditing

There are two options available to use when auditing; a quick audit or a full scan with an option to schedule your scans. Ideal for those who want to put it into the server room and then to perform a monthly audit of the servers or certain parts of the network. This is also an excellent option for those of you that want to be able to offer this as a managed service to your clients. You are also able to see trends on the audits by comparing each scan against the others that have happened in the past.

Quick Audit

This is a small basic audit that scans the known TCP ports and then performs checks against 20 known vulnerabilities to see if your system is susceptible.

Full Scan

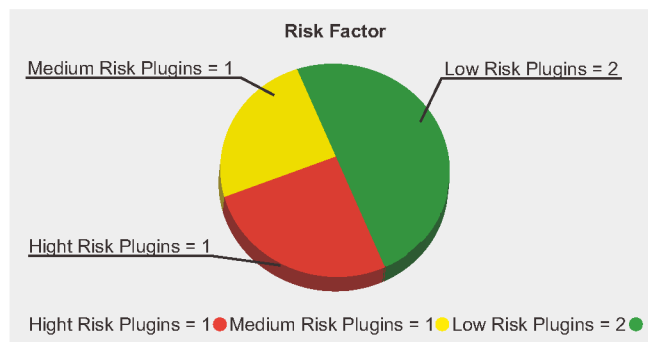
The full scan option will perform an assessment of your requested systems, you have the option to enhance this audit by allowing the system to actually deliver the payload against the machines in question. The Penetrator database of vulnerabilities is currently in excess of 42,000 and is continually growing, as you receive updates throughout the day. Once the audit has completed you are presented with the options on how you would like to view the results.

Reporting

There are two main report options available to you; the Executive summary or the full report (including solutions to the vulnerabilities it has identified). The Executive summary is aimed at the management types and provides enough information concerning the audit, including graphical detail and the amount of vulnerabilities found.

The full scan goes into a lot further detail with information on each vulnerability found and a resolution on how to prevent this from being exploited in the future.

An overall risk factor graphic is provided which gives you an immediate indication as to how secure or insecure you are.



You are able to customise and personalise the reporting so that you can insert your own company logo etc which will enable you to sell these to your customers (this is permitted within the licencing of the unit).

Overall Impressions

Whether you are a professional tester or just starting out this unit is a complete solution for testing your own or your customers' networks. Its ease of use is a serious advantage as you wouldn't need to spend time and effort in configuring the system up etc apart from the initial wizards. Once you have scheduled all your audits, you can tuck it away somewhere and forget about it, although you could have it sitting under your desk and would never know it was there, as its almost silent operation had myself checking on more than one occasion to ensure it was turned on.

The sensible clear layout of the menu's makes it so simple to use, that even complete beginners will be using this within 15 minutes. The help documentation provided is of first rate and clear about what you need to do for each section. If you're not the "manual" type each section has a video tutorial attached to it as well.

Finally I have to say something about the support I received when I had some difficulties with my unit. I can sum it up in one word. Superb! They were very quick on their initial response and kept me up-to date throughout the issue. Even offering to remote in to the machine to double check that I hadn't made a simple mistake. Once it was all resolved, they still followed up the next day to ensure I was still working properly. This has got to be one of the best levels of support I have received in a very very long time.

URL: <http://www.secpoint.com/penetrator.html>
 Product SP-S300-8-1YB
 Price (Euro's)949.00