

The Penetrator IT Security Review



ΔΙΜΗΝΙΑΙΟ ΠΕΡΙΟΔΙΚΟ για την ΑΣΦΑΛΕΙΑ των ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ

“The Penetrator is sold completely installed with the all essential applications and modules and it is ready for use.”

“One of the basic characteristics is the friendliness of use through flexibly menus, that achieves fast familiarization with the operation system.”

“The appliance also has the ability to connect many Penetrators in a distributed network, something that provides a lot of advantages such as central submission of reports, central evaluation”

“Consider that the newest available automated hacking tools can cause big damage in an enterprise network in a minimal of time, that is why classifies vulnerability evaluation as basic priority in any strategy of IT safety. In this situation Penetrator is very usefully solution that was developed by 'SecPoint' and distributed in our country by K & G Digital Service Ltd. It is an appliance of testing, evaluation and infiltration for vulnerabilities on any network.

The Penetrator is sold completely installed with the all essential applications and modules and it is ready for use. The cost is particular accessible, while the value can be proved incalculable, because only one potential infiltration from a hacker in the network will allow access in the critical data, it can be proved devastating. Penetrator therefore, not only detects vulnerabilities in a network, but at the same time proposes solutions for each problem separate.

One of the basic characteristics is the friendliness of use through flexibly menus, that achieves fast familiarization with the operation system.

Attempting to report some of the basic attributes of Penetrator, it deserves to point out that initially the 11.000 installed signatures in the database, so that is provided complete knowledge of vulnerabilities of the network. The signature database is updating many times over a daily base. Also, with Penetrator the administrator can run real exploits (attacks) so that he can checks that a certain vulnerability is exploitable. It is also possible to run real "Denial of Service" attacks in pre-production systems, for control and testing of their stability. The appliance also has the ability to connect many Penetrators in a distributed network, something that provides a lot of advantages such as central submission of reports, central evaluation and central point of readjustments. Besides, it can detect any functional system and appliance in the network, something that is particularly beneficial from the moment where it has the possibility of detecting vulnerabilities in any appliance and device in the organisation.

All Penetrators support connection of many users. This can be used in order to have different accounts, with different addresses [IPs] to detect. At the same time, it allows the tackling of the reports and the personalize for each user report separately. SecPoint has also a portable Penetrator, which provides evaluation of wireless networks (WEP, WPA and WPA2) . This is a success with the real cracking precisely as a hacker would act.

External Links:

http://www.securitymanager.gr/it_security/sub/review_pdf/penetrator.pdf