WiFi Penetration Testing - Wireless Auditing

The Portable Penetrator allows you to do real WiFi Penetration Testing WEP, WPA, WPA2 & WPS auditing. Just like an attacker would do it! It highlights any weaknesses in wireless networks and shows how these can be secured most effectively.

60.000+ Database Signatures

The Penetrator vulnerability database consists of more than 20 years of research. The database contains more than 60.000+ unique vulnerabilities ready to identify any vulnerability in your network. This database is updated multiple times daily.

Launch Real Exploits and Denial of Service Attacks

You can launch real exploits to verify that an identified vulnerability is exploitable. It is also possible to launch real Denial of Service attacks to test preproduction systems for stability.

Reports Branding

Branding and personalisation of the reports and selling them as a service is allowed.

Whether you're a security professional or a novice, Portable Penetrator PP3000 is a device which is a complete solution for auditing and improving the level of security of wireless networks. Thanks to built-in report module you will have all the documentation of the security audits you have conducted. The product has a great value for a great value for a complete solution like Portable Penetrator PP3000.
Features

Security Audit Features
- Vulnerability assessment
- 60,000+ signatures
- Unlimited auditing
- Works out of the box
- Advanced auditing options
- Launch real exploits
- Audit any OS
- Automatic web crawl script
- OS independent interface
- SANS top 20 audit

Vulnerability Assessment & Ticket System
- Easy-to-understand reporting
  - XML PDF and HTML reports
  - Reports branding allowed
  - Option for syslog remote logging

Wireless Auditing
- Finds cross site scripting
- SQL injection and web errors

Automatic database and software updates
- Scalable and Upgradeable
  - Automatic database and software updates
- Support and Maintenance
  - One year database subscription included
  - Full support included in price
  - Web-based User Interface (https)
  - Quick setup wizard
  - Configuration backup/restore
  - Email alert and logging via syslog
  - Built-in diagnostic function
  - Fast Live Chat Support
  - Ticket System Support

Scheduled Auditing
- Security Audit Configuration
  - Virtual host auditing
  - Audit specific ports
  - Audit specific web directories
  - Get an email when an audit is finished

Penetration Testing
- Launch real exploits for Windows®, Unix®, Routers, Firewalls and more.
- Launch real denial of service attacks

Automatic Update
- Automatic daily database updates
- Automatic firmware updates with new features and functionality
- Centralized update point

Specs

<table>
<thead>
<tr>
<th>Features</th>
<th>SecPoint® Portable Penetrator™ PP2000</th>
<th>SecPoint® Portable Penetrator™ PP4000</th>
<th>SecPoint® Portable Penetrator™ PP6000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Scanning Capacity</td>
<td>1-4 IPs</td>
<td>8 IPs</td>
<td>16-2048 IPs</td>
</tr>
<tr>
<td>Vulnerability Assessment &amp; Ticket System</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Runs Virtually on Windows / Mac OS X</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>10 Profiles HIPAA, Firewall, Agressive and more</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>60,000+ Database Signatures</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Launch Real Exploits &amp; Denial of Service</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Allowed to Change IP Addresses</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Distributed Security Auditing</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Automatic database and software updates</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>