

AppDetectivePro™

Evaluation

AppDetectivePro is a complete database assessment and audit solution offered by Application Security, Inc.

This Evaluation Guide demonstrates how to load the software on a test box, how to find the vulnerabilities present on a target unit under test, how to review the access rights of users on a target unit under test, and how to report on all issues found.

This basic evaluation should take 30 minutes. After completing it, you may want to explore more of what AppDetectivePro has to offer, like reviewing the Policy Editor and understanding all the possible checks that can be run against your databases.

1 **DOWNLOAD** Get a copy of AppDetectivePro for evaluation

Download AppDetectivePro by completing the web form found at: appsecinc.com/downloads/. You will receive instructions on how to put a self-extracting executable to your test box. The test box minimum requirements include: Windows XP, Vista or 7 (English), 2GB of RAM, and 400MB of disk space for installation. The default install is recommended to streamline evaluations.

NOTES:

- You may need to rename the file to appdetective_setup.exe.
- You must run the install as an Administrator.
- You can choose to install a Microsoft SQL Server 2008 R2 Express instance or supply your own for the installation.
- The license accompanying the evaluation version enables a Pen Test, an Audit, and User Rights Review of ONE unit under test (per database type), and locks the test scenario to the DOWNLOAD policy, or set of tests.
- Access to the Policy Editor is disabled on evaluation software.
- The ASAP Update feature is disabled on evaluation software.
- All reports generated will contain "Evaluation" within the report.
- The evaluation period lasts for 30 days from the first time you run AppDetectivePro.

2 **DISCOVERY** Scan a segment of the network to discover what database instances are present

Click the "Discover" button on the AppDetectivePro tool bar. A wizard will step you through the process of creating a new session.

NOTES:

- Scanning a Class C network (255 addresses) with 12 live hosts, looking at the default ports of all the listed applications will take approximately 6 minutes.
- Scanning a larger network or a more extensive list of ports will take longer. The number of dead IP/Port combinations and network latency also can impact the Discovery scan time.
- While the Discovery scan is running, a progress monitor dialog box appears that gives you the capacity to "Stop" the scan. If you choose to stop the scan, the results already gathered will be displayed in the network tree

When the Discovery is complete, the progress monitor dialog box disappears. The left hand display frame displays a categorized list of the discovered databases on the inventoried network. Expand the tree in the left hand frame to view the discovered databases and applications. Click on an item in the tree, and select the "Details" tab in the right hand display frame to gather the application's banner data—a summary of the vendor and release information.

3 **PEN TEST** Select a database and assess its vulnerability to EXTERNAL attack

Click the "Pen Test" button on the AppDetectivePro tool bar. The RUN PEN TEST dialog box will appear and display the database inventory list. Choose a unit to test by selecting the desired instance. The default "Policy to Use" box will be set to "Download (Built-in)"—a set of tests, or policy, that illustrates AppDetectivePro's capabilities. The fully licensed version of AppDetectivePro includes not only a range of pre-built policies but allows the creation of custom policies via the "Policy" button on the tool bar. Click "Run Pen Test." The progress monitor dialog box will appear, enumerating each test and check as it is performed. A "Stop" button is available.

NOTES:

- A Pen Test policy may include checks to assess password strength. Dictionary attacks may be time consuming. If a policy that contains password checks is used, a warning pop-up will display stating that accounts maybe locked. You can proceed to continue with the Pen Test or not.

Upon completion of the Pen Test, a list of vulnerabilities sorted by severity appears in the bottom display frame, one vulnerability per line. Select one of the vulnerabilities from the bottom pane. In the right-hand display frame under the "Vulnerability Description" tab, you will see details, including fix information, for the vulnerability.

4 AUDIT

Select a database and run an authenticated scan to identify vulnerability to INTERNAL attack and misuse

Click the "Audit" button on the AppDetectivePro tool bar. The CHOOSE APPLICATIONS TO AUDIT dialog box will appear displaying the inventory of discovered databases. Choose a unit to test by checking the desired application instance. Click "Audit Applications" and the RUN AUDIT dialog box will appear. Click in the "Audit Information" box, and enter an authorized database Username and Password when prompted. Also enter a valid OS Username and Password, if OS checks are enabled. You can test the connection to the database and the OS by clicking the "Test DB Connect" and "Test Login" buttons.

NOTES:

- To run an Audit you must have an account on the unit under test. Reference the Appendix in the Online Help for the READ ONLY permissions needed.
- To Audit Sybase ASE, IBM DB2, MySQL or Lotus Domino, you must have client drivers loaded on the test box

The "Policy to Use" box will be set to "Download (Built-in)." Click "Run Audit." The progress monitor dialog box appears, enumerating each test and check as it is performed. A "Stop" button is available.

NOTE:

- An Audit policy may include password and permissions granted checks. The total duration of the Audit scan has a variable on the number of database users and the number of password and permissions granted checks enabled.

Upon completion of the Audit, the prioritized list of vulnerabilities in the bottom display frame will include the additional vulnerabilities uncovered by the Audit test.

5 WORK PLAN

Import a work plan and see how the scan results provide evidence to answering your audit control questions

Click "Tools" from the AppDetectivePro task menu and "Import Questionnaire." The IMPORT QUESTIONNAIRE dialog box will appear. Click the "Browse" button and select the "Questionnaire_GenericDemo" file to open. Click the "Import" button. This will import the file, show you progress of the import, and give you a confirmation upon completion. Once the file is imported, close out of the IMPORT QUESTIONNAIRE dialog box.

Click the "Interview" button on the AppDetectivePro tool bar. The CHOOSE AN AUDIT AND QUESTIONNAIRE WORK PLAN TO INTERVIEW dialog box will appear displaying the inventory of discovered databases and associated scan results. Choose an audit result to perform the interview by checking the box. Click "Run Interview" and the INTERVIEW dialog box will appear. Click the "Start Interview" button and proceed answering the form. Use the "Next" and "Previous" buttons to select the question to answer. When finished, click "Finish Interview." Once completely finished and closed, you will not be able to reopen it and change any answers. You can choose to "Continue Later," and edit the interview as well.

6 USER RIGHTS REVIEW

Select a database and take a snapshot of all the permission relationships between Users, Roles, and Objects

Click the "User Rights" button on the AppDetectivePro tool bar. The CHOOSE APPLICATIONS TO RUN USER RIGHTS REVIEW dialog box will appear displaying the inventory of discovered databases. Choose a unit to test by checking the desired application instance. Click "Run Review" and the RUN USER RIGHTS REVIEW dialog box will appear. Click in the "User Rights Review Parameters" box, and enter an authorized database Username and Password when prompted. You can test the connection to the database by clicking the "Test DB Connect" button.

NOTE:

- To run a User Rights Review you must have an account on the unit under test. Reference the Appendix in the Online Help for the READ ONLY permissions needed.

Click "Run Review." The progress monitor dialog box appears, providing status of the snapshot collection. A "Stop" button is available.

Upon completion of the User Rights Review scan, navigate the network tree to the unit the scan was performed on and click on the User Rights Review scan icon. On the "Details" tab, you will find information about the number of users and roles identified and all database parameters.

7 REPORT

Produce actionable reports of the scan results

Click the "Reports" button on the AppDetectivePro tool bar to access a set of dialog boxes that will guide you through report creation. The reports are available in a number of formats for local viewing or for export. Canned reports are grouped by Audit and Pen Test and User Rights Review.

For a quick view of vulnerability results, choose the Vulnerability Summary report and follow the rest of the report wizard. The Check Status report also provides you the information of what check was performed and if a violation was found or not.

To quickly report on the effective rights of a user in the database, choose the All Effective Privileges for a User report. Follow the report wizard, select the user, and run the report. The Object Access report gives you a report on what user or role has access to the object and what type of access it is.

To explore more of what AppDetectivePro has to offer, understand its pricing model, and more, contact: sales@appsecinc.com.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

Follow us on Twitter: www.twitter.com/appsecinc | www.twitter.com/teamshatter

**APPLICATION
SECURITY, INC.®**

www.appsecinc.com