

Результаты тестирования шлюза x2500 под управлением m150

Тестирование провёл: Pete Kuzeev, Security Presale Engineer, RRC Moscow



Благодарности: Thomas Drews - Sr. Systems Engineer
Barry Shteiman, Johan Nordstrom, Alexander Kolybelnikov

Поскольку основной акцент при использовании системы делается на защиту СУБД, то в первую очередь были отмечены самые популярные из них на сегодняшний день – **MS SQL, Oracle, IBM DB2 и MySQL**



Одним из наиболее критичных приложений для деятельности организаций, работающих с данными СУБД, является **1С** – поэтому часть тестов пришлась и данное ПО

Многие используют порталы для внешних и внутренних корпоративных ресурсов, даже у 1С есть веб-сервисы, поэтому мы также добавили на стенд самую популярную связку **Apache + PHP + MySQL**



Традиционно весьма уязвимая, но работающая на многих системах без ведома администраторов MS IIS в связке **Web + Ftp**

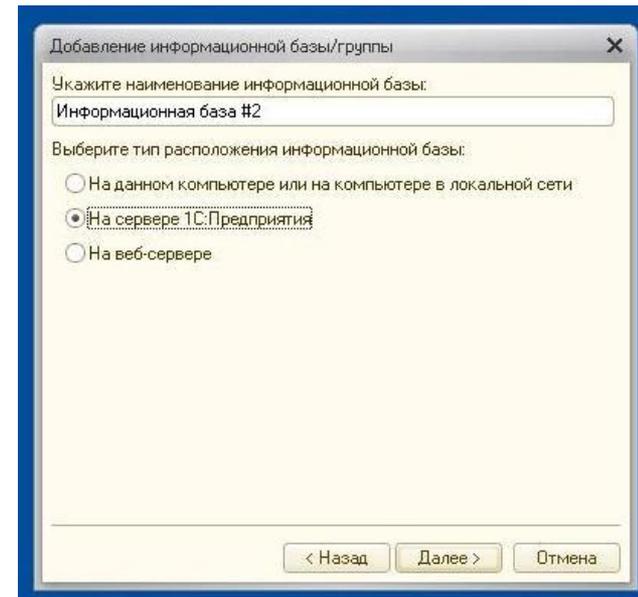
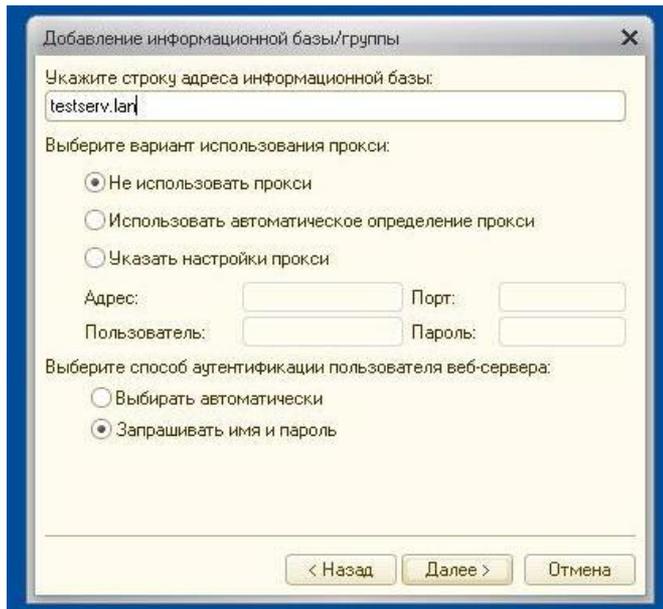
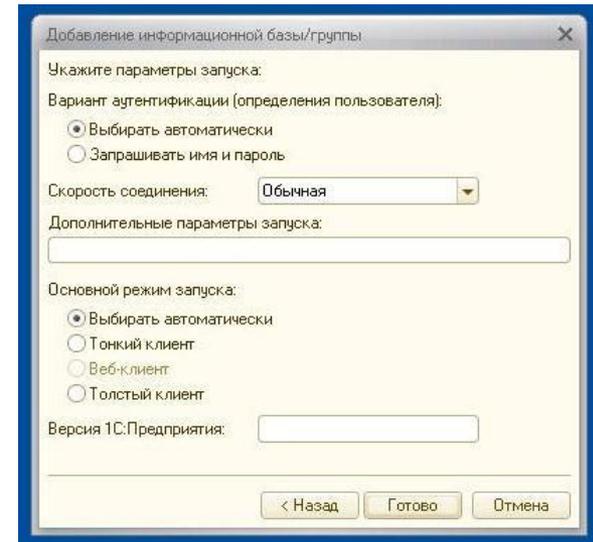
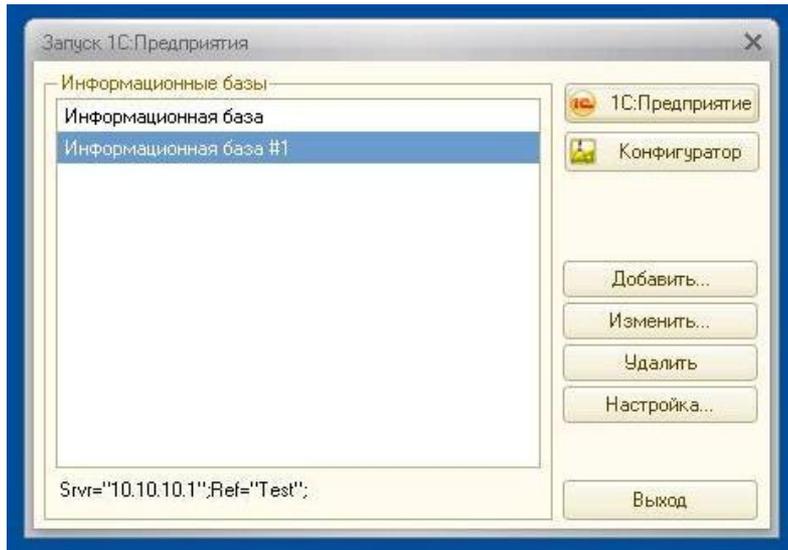
Системы автоматизированного проектирования уже давно обрели статус систем способных «освоить» любые мощности и период, когда для хранения своих данных они довольствовались локальными таблицами и библиотеками в прошлом – **SAP + Oracle**

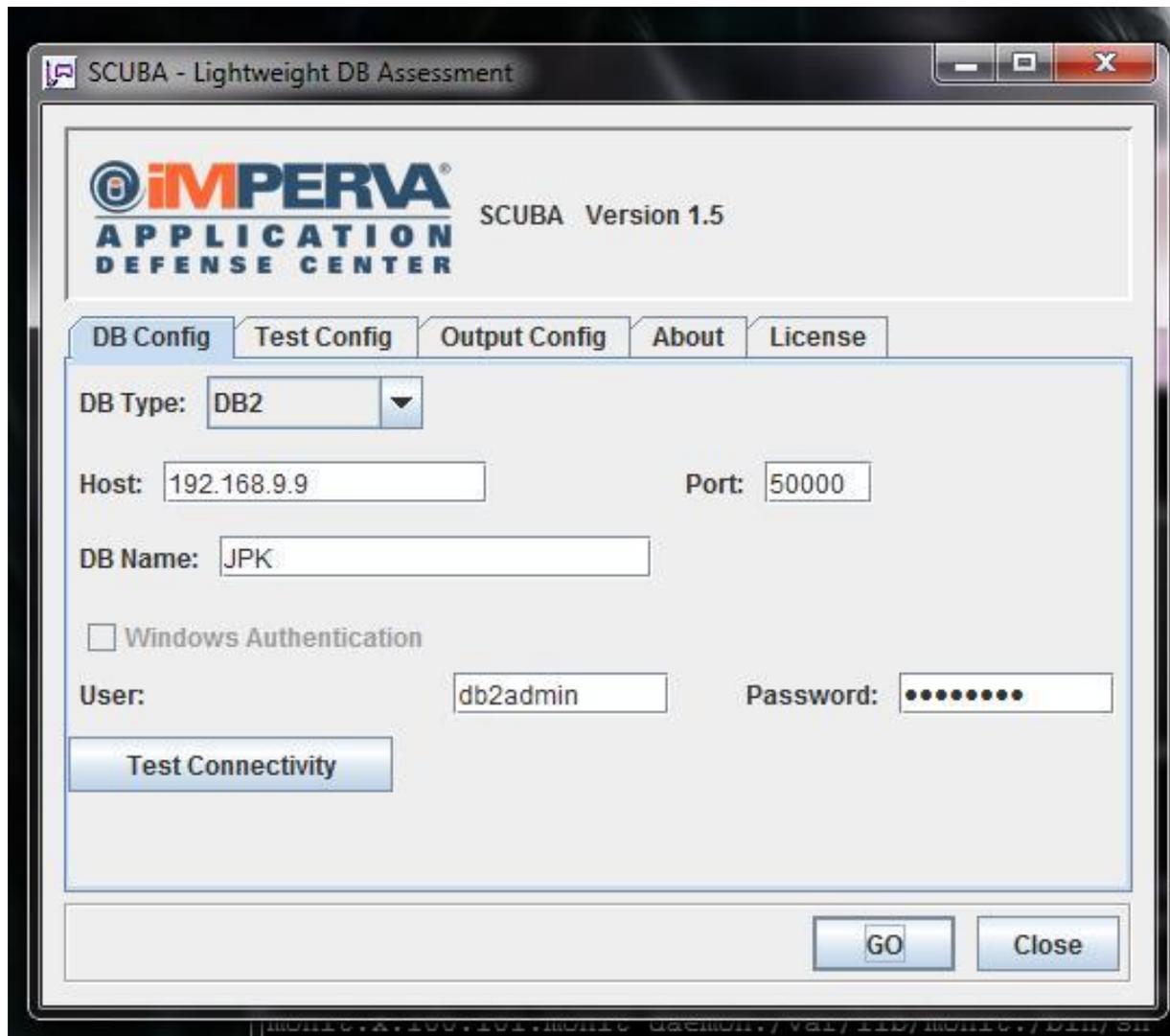
User Defined Data Interfaces

	Service Type	 	Interface Type	Service	Ignore	Last Packet
	Http		TCP	Default Si... - 192.168.9... - Http	<input type="checkbox"/>	None
	Db2		TCP	Default Si... - 192.168.9... - Db2	<input type="checkbox"/>	None
	MySql		TCP	Default Si... - 192.168.9... - MySql	<input type="checkbox"/>	None
	Http		TCP		<input type="checkbox"/>	

Http

- Http
- Oracle
- MsSql
- Sybase
- Db2
- Informix
- Teradata
- SybaseIQ
- MySql
- Netezza
- Progress





SCUBA – сканер уязвимостей СУБД от Imperva

Retina, X-Spider, Nessus, Acunetix – сканеры уязвимостей

NeXpose – сканер уязвимостей с динамикой (flood)

SQL Stripes – система мониторинга

ERPSsan – сканер уязвимостей SAP

Помимо всего выше перечисленного, позволяющего получить некоторые данные в автоматизированном режиме, был использован ряд утилит и множество скриптов на Perl написанных под конкретные задачи или популярные уязвимости...

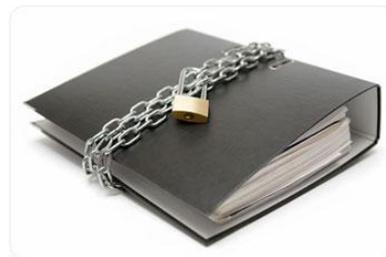
Список тестируемого ПО – MS SQL 2008/2005, Oracle 11g Express, IBM DB2 9.7.4 Express, Apache 2.1, PHP 5.0, MySQL 5.1, 1C 8.2, SAP R3 4.6D r8



Стенд состоял из двух устройств от Imperva – шлюз x2500 и сервер управления m150, использовалось три подсети – одна для управления сервером, вторая для работы сервера и шлюза и третья для защищаемых сервисов

Хочу обратить ваше внимание на то, что мы использовали шлюз в режиме прозрачного моста, т.е. рассмотрен самый оптимальный вариант, когда для внедрения устройства не требуется вносить никаких изменения в рабочую сетевую инфраструктуру

Сервисы были установлены как реальных, так и на виртуальных машинах, особой разницы в тестах, кроме ожидаемых временных задержек мы не обнаружили

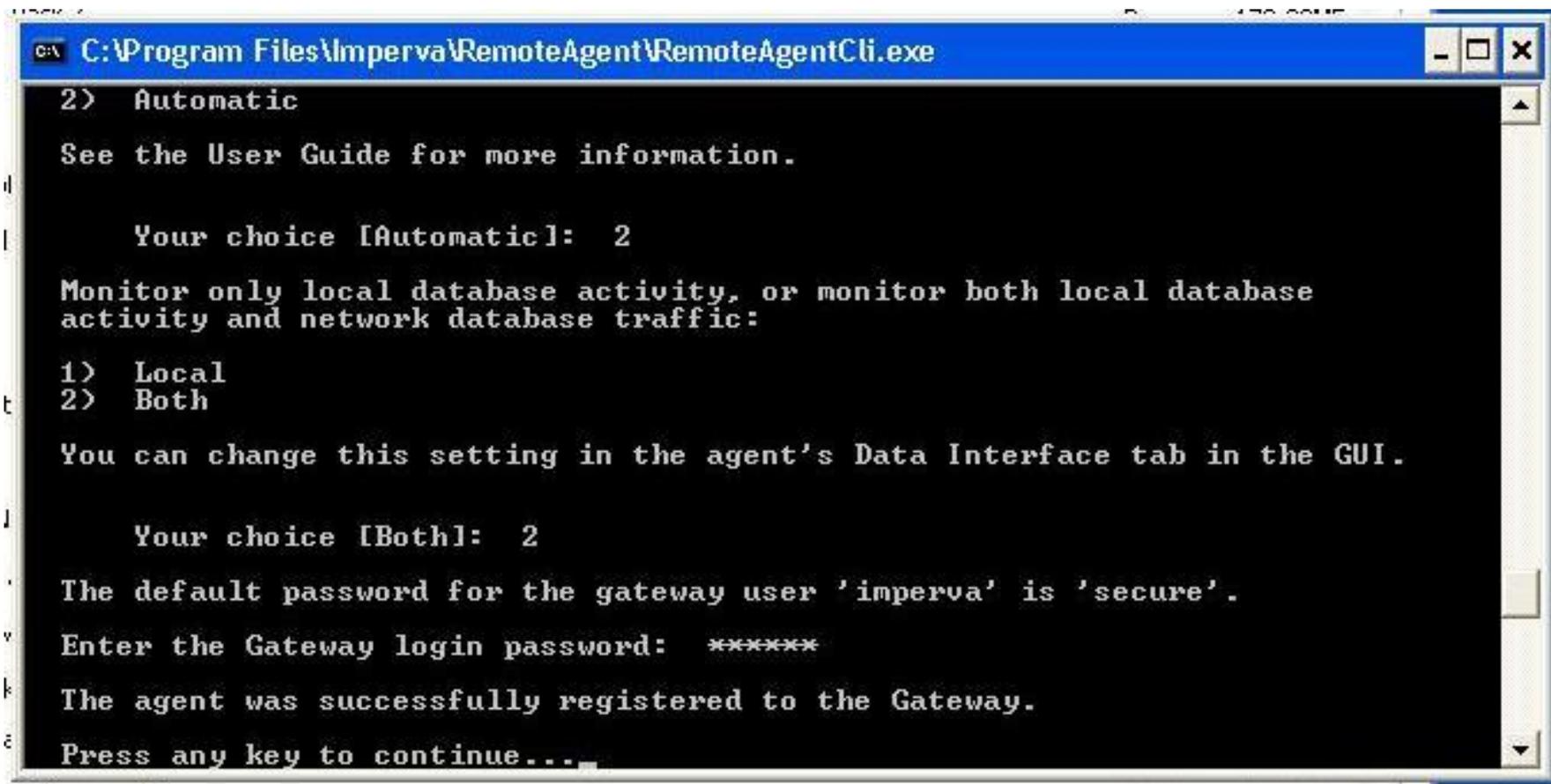


По умолчанию работа комплекса ограничивается установкой и настройкой самих устройств без нагрузки защищаемых клиентов каким-либо дополнительным ПО, но существуют ситуации, при которых, установка клиента (в нашем случае – Imperva Agent) является единственным вариантом для получения тех или иных данных , например – загрузка ЦП

Imperva Agent – решение клиента в виде сервиса с весьма скромными требованиями к целевой системе, его присутствие в ней не замедляет работу и не затрудняет взаимодействие развёрнутых сервисов

Администрировать комплекс можно через защищённый веб-интерфейс, который доступен через специальные порты управления. Стандартный доступ по SSH, а также отдельный консольный порт, поддерживающие режимы native unix - для основных системных настроек





```
C:\Program Files\Imperva\RemoteAgent\RemoteAgentCli.exe
2) Automatic
See the User Guide for more information.

Your choice [Automatic]: 2
Monitor only local database activity, or monitor both local database
activity and network database traffic:
1) Local
2) Both
You can change this setting in the agent's Data Interface tab in the GUI.

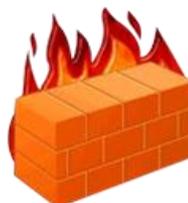
Your choice [Both]: 2
The default password for the gateway user 'imperva' is 'secure'.
Enter the Gateway login password: *****
The agent was successfully registered to the Gateway.
Press any key to continue...
```

```
root@impervamx:~  
-----  
SecureSphere 8.0.0.8265 - impcfg Top Screen  
-----  
Configuration target:      local (appliance, M150, reachable)  
Management server status: running,Ready  
Setting markers:          C: changed, I: invalid, P: pending (saved but not applied)  
Navigation:               Top  
  
Management server settings  
  'secure' user password:  <is-set>  
  'system' (database) password: <is-set>  
  
1) Manage SecureSphere Management Server.  
2) Manage SecureSphere Gateway.  
3) Manage platform.  
4) Upgrades/updates.  
  
s) Show changes.  
D) Discard changes.  
  
S) Save settings.  
A) Apply settings.  
T) Change configuration target.  
q) Quit (discarding not-saved changes).  
  
Your choice: █
```

Когда на в руки попадает «красивая вещь» – первым делом приходит мысль о такой полезной функции, как конфигурация по умолчанию. Хочется распаковать апплайнс и проведя начальное конфигурирование получить более менее рабочую систему, так мы и поступим

Собрали и настроили стенд по описанию, данному ранее, и запустили предварительное сканирование тестовой защищаемой машинки из двух подсетей – внешней (подразумеваем интернет) и подсети управления, через которую мы тоже можем постучать на защищаемую машинку

На следующем слайде приведены результаты сканирования одной из программ, если заметить в целом, то первое впечатление о политиках безопасности по умолчанию – очень хорошее, из подсети управления, которая считается доверенной, все соединения по поиску средних и высоких по опасности уязвимостей разрешаются это видно в сканере и апплайнс просто информирует нас, о таких попытках, из общественной сети – все данные соединения отсеиваются шлюзом, без каких-либо дополнительных настроек



The screenshot shows the XSpider 7.7 interface. The left pane displays a scan tree for IP 192.168.9.9. The entry 'Удаленное выполнение команд (ms04-035)' is highlighted. The right pane shows a detailed alert:

Подозрение на серьезную уязвимость
Удаленное выполнение команд (ms04-035)

Описание

Уязвимость обнаружена при выполнении Domain Name System (DNS) преобразования в Windows Server 2003 SMTP компоненте. Удаленный атакующий может заставить сервер обработать частичный DNS запрос, чтобы выполнить произвольный код на уязвимой системе с SYSTEM привилегиями. Уязвимость также существует в Microsoft Exchange Server 2003 Routing Engine компоненте на Microsoft Windows 2000 Service Pack 3 или на Microsoft Windows 2000 Service Pack 4.

Решение

Установите обновление:
<http://www.microsoft.com/technet/security/bulletin/MS04-035.msp>

At the bottom, the status bar shows 'Сканирование' (Scanning) and the IP address '192.168.9.9'.

Удачные попытки сканирования из доверенной сети

Задача1 (Default.prj) - XSpider 7.7 Demo Build 3100

Файл Правка Вид Профиль Сканирование Сервис Окно Справка

Сканируемые hosts (1)

- 192.168.9.9 [SECURITY-NOTE] (128)
 - Система
 - 21 / tcp - FTP
 - 25 / tcp - SMTP
 - Удаленное выполнение команд (ms04-035)
 - 80 / tcp - HTTP
 - 123 / udp - NTP
 - 135 / tcp - RPC Windows
 - 137 / udp - NetBIOS Name
 - 139 / tcp - NetBIOS
 - 445 / tcp - Microsoft DS
 - 912 / tcp - VMware Authentication
 - 1044 / tcp - RPC Windows
 - 1068 / tcp - RPC Windows
 - 1540 / tcp - rds
 - 1541 / tcp - rds2
 - 1560 / tcp - asci-val
 - 3306 / tcp - MySQL
 - 3389 / tcp - MsRDP
 - Подмена данных**
 - Информация RDP
 - Удалённое управление
 - 6129 / tcp - DameWare Mini RC

Уязвимость
Подмена данных

Описание

Краткое описание

Уязвимость позволяет атакующему подменять открытые ключи доверенных серверов и проводить атаки типа "человек-посередине".

Подробное описание

При использовании протокола Remote Desktop Protocol (RDP) в Microsoft Terminal Server закрытые ключи RSA хранятся в mstlsapi.dll и используются для подписывания сертификатов, что позволяет злоумышленникам, действующим удаленно, подменять открытые ключи доверенных серверов и проводить атаки типа "человек-посередине".

Для успешной эксплуатации злоумышленнику необходима возможность перехватывать трафик между терминальным сервером и терминальным клиентом.

Ключ использованный для подписи сертификата:

```
-----BEGIN RSA PRIVATE KEY-----
MIBPQJBAAJBAIfqbQVfCZMgu2H1GgkGXmx9XPY9/r/nfO/+OlhrZWPOIUVS8ppr
t9fiwfxvhyCIPstfukoewbtNyT5Dcr1eOj0CBQDAiHtbAkBf8z/nEwEQx70buQsX
eQc13Q17CrG6x5kksd0knxKaF2A16JkzzJLPIEin6fmpIT4aGUILFhYAWFWHEdoy
GaeHAIEA65VvxlhX8FVXIKOrRirB6pXkMRbB3/cH8TvSVyApvT8CIQCTscvEWZqD
RXjW5wNqX4NSsN8+QwJtJ6bWrED0J3dgwIhAKbZfTYPTIDhuGOtY6NqhnJhWGZ5
XCa5finNF0joQ51AIBuBd5gKaodJ5DMI/X/CQNa897sxhxZzdcO9l8Bwu8/dQIh
AKs1m+mbW0TfDH7GxSpfQHvknM+IO/Dq59VzZnvHXDhfa
-----END RSA PRIVATE KEY-----
```

Уязвимые версии

- Windows 2000
- Windows XP
- Windows 2003 Server
- Windows Vista
- Windows 2008 Server

Использование уязвимости

Использование уязвимости удаленно: да
Использование уязвимости локально: да

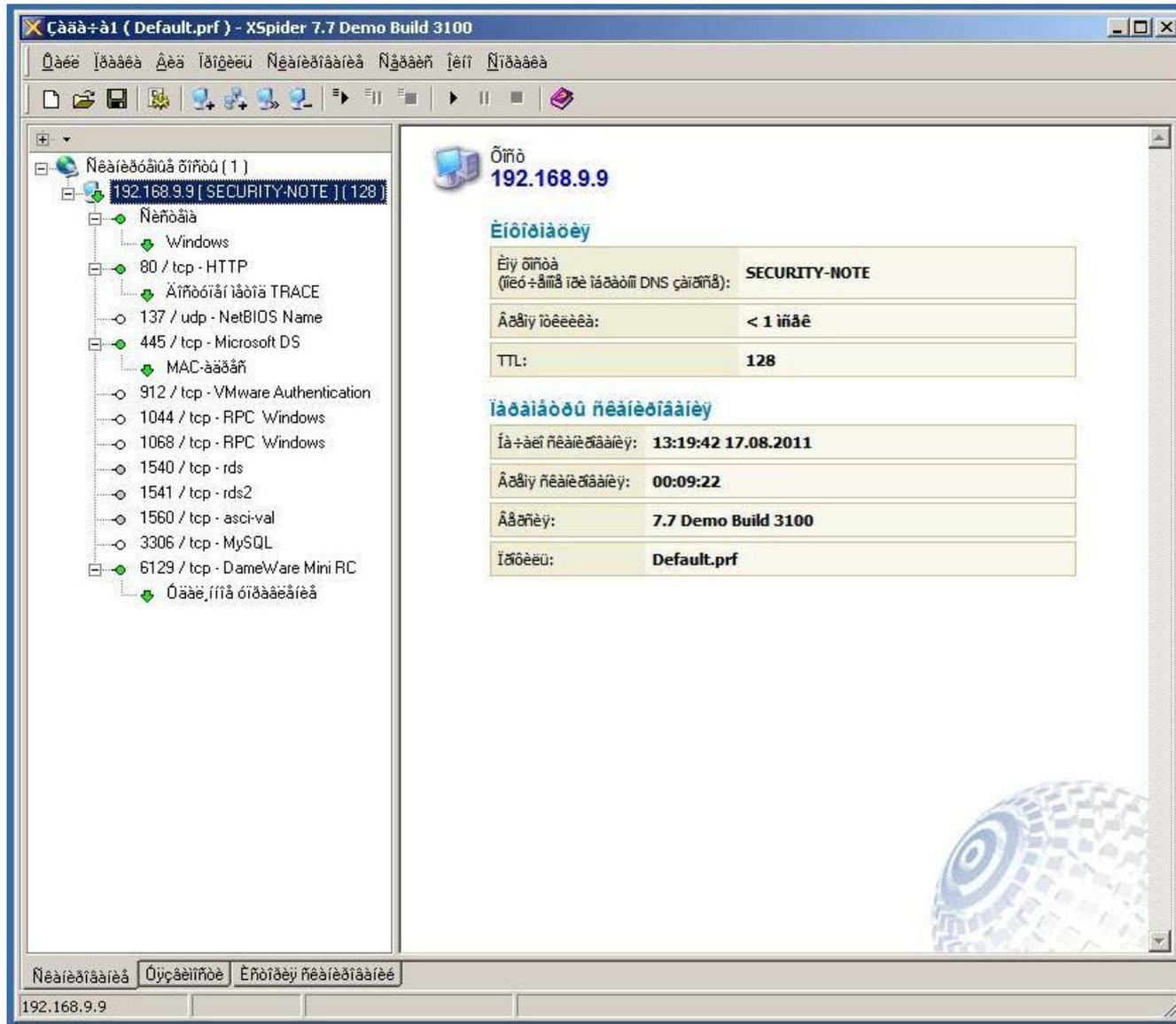
Базовая оценка по системе CVSS v2

CVSS Base Score: 5.1
(AV:N/AC:H/Au:N/C:P/I:P/A:P)

Сканирование Уязвимости История сканирований

192.168.9.9

Удачные попытки сканирования из доверенной сети



Попытки сканирования из небезопасной сети – критичные уязвимости отфильтрованы

Поскольку основное направление нашего тестирования СУБД – вторым пунктом в наших тестах стояли именно они, маленькая ремарка, для тестов были применены политики предлагаемые системой как оптимальные для защиты наших сервисов, т.е. мне не нужно было тратить большое количество времени на оставление карты потенциальных уязвимостей

Хочу отметить самые важные тесты в области защиты СУБД - это создание запроса, позволяющего извлечь любые системные данные, обойти проверку пользователя при доступ к определённым таблицам, а также для некоторых СУБД (например, Oracle) получить доступ к файловой системе и произвести загрузку некоторого исполняемого кода, для получения полного доступа к системе

Тестировались как БД созданные нами, так и БД созданные 1С и SAP R3 – в обоих случаях ни один из целевых запросов, эксплуатирующих критичные уязвимости не вошёл за границы защищаемого шлюзом Imperva периметра, на наш взгляд - **это отличная перспектива забыть о постоянных обновлениях и патчах для СУБД, которые порой снижают её производительность, а также получить великолепную систему мониторинга и оповещения**

IMPERVA SECURESPHERE | Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | Threat Radar

Dashboard | Alerts | Violations | System Events | Blocked Sources

Main | Admin | Preferences | Tasks | Log out | Help

View | Save As | Actions

Quick Filter

Basic Filter | Saved Filters

By Severity

- Informative
- Low
- Medium
- High

By Event Type

- http
- sql
- network
- file

By Alert Type

- Firewall
- Signature
- Protocol
- Profile
- Worm
- Correlation
- Custom

By Alert Number

By Server Group

- 192.168.9.X

By Service

- MySql (192.168.9.X)
- Http (192.168.9.X)
- Oracle (192.168.9.X)
- Db2 (192.168.9.X)
- MsSQL (192.168.9.X)

By Application

- Default Oracle Application (O
- Default MySql Application (My
- Default MsSql Application (Ms
- Default DB2 Application (Db2)

Apply | Save | Clear

Advanced

Violations (filtered)

Time	Alert ID	Severity	Event Type	Alert Type	Server Group	Service	Application	Description
00:25:13	...4158	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Suspicious Response	Suspicious Response
00:24:41	...4156	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Suspicious Response	Suspicious Response
00:06:33	...2894	High	sql	Unauthorized Access	192.168.9.9	192.168.10.227	Unauthorized Access	Unauthorized Access
00:06:30	...2893	High	sql	Unauthorized Access	192.168.9.9	192.168.10.227	Unauthorized Access	Unauthorized Access
00:01:46	...2243	High	sql	Unauthorized Access	192.168.9.9	192.168.9.255	Unauthorized Access	Unauthorized Access
00:00:30	...1798	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1797	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1796	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1795	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1794	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1792	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1791	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1790	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1789	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1788	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1787	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1786	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1784	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1783	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1782	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1780	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1779	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1777	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1775	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1774	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1773	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1771	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1770	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1769	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1768	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1767	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1766	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1765	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1764	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
00:00:30	...1763	High	sql	Excessive Attempts o	192.168.10.227	192.168.9.9	Excessive Attempts o	Excessive Attempts o
8/23/11	...1756	High	sql	Unauthorized Access	192.168.9.9	192.168.9.255	Unauthorized Access	Unauthorized Access
8/23/11	...1613	High	sql	Unauthorized Access	192.168.9.9	192.168.9.255	Unauthorized Access	Unauthorized Access
8/23/11	...1612	High	sql	Unauthorized Access	192.168.9.9	192.168.9.255	Unauthorized Access	Unauthorized Access
8/23/11	...1611	High	sql	Unauthorized Access	192.168.9.9	192.168.10.227	Unauthorized Access	Unauthorized Access
8/23/11	...1610	High	sql	Unauthorized Access	192.168.9.9	192.168.10.227	Unauthorized Access	Unauthorized Access
8/23/11	...1609	High	sql	Unauthorized Access	192.168.9.9	192.168.10.227	Unauthorized Access	Unauthorized Access
8/23/11	...1608	High	sql	Unauthorized Access	192.168.9.217	192.168.9.255	Unauthorized Access	Unauthorized Access
8/23/11	...1607	High	sql	Unauthorized Access	192.168.9.217	192.168.9.255	Unauthorized Access	Unauthorized Access
8/23/11	...1606	High	sql	Unauthorized Access	192.168.9.9	192.168.9.255	Unauthorized Access	Unauthorized Access
8/23/11	...1603	High	sql	Unauthorized Access	192.168.9.9	172.18.10.176	Unauthorized Access	Unauthorized Access

Event 8883620053359001770: Excessive Attempts of Database Login

Details

Excessive Attempts of Database Login

Event 8883620053359001770: Excessive Attempts of Database Login

Key	Value
Violation Type	sql
Severity	High
Policy Name	SQL Correlation Policy
Alert Number	2004
Violation Description	Excessive Attempts of Database Login by
Violated Item	User: jpk
Immediate Action	None
Number of Login Attempts	13
Allowed Number of Attempts	5

Event Details:

Event Time: August 24, 2011 12:00:30 AM | Gateway: impervact

Server Group	Service	Application
192.168.9.X	Db2	Default DB2 Application

Connection	User	DB Application	OS User
192.168.10.227:46371 → 192.168.9.9:50000	jpk	db2jccawt-eventqueue	

Affected Rows	Response Size	Response Time
0	0 Records	3 msec.

Error Code	Error Message
0	

Databases and Schemas:

Database	Schema
jpk	jpk

Privileged Operations & Stored Procedures:

Operation	Objects	Type
No data found		

Table Groups:

Table Group Name	Black List	Sensit
No data found		

Source Application Details:

Application Name	db2jccawt-eventqueue
Application User	
Web Session ID	None
Source URL	N/A
Web Client IP	N/A
Web Event ID	N/A

Additional Info:

Normalized Query	N/A (login)
------------------	-------------

IMPERVA SECURESPHERE | Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | **Monitor** | ThreatRadar

Dashboard | Alerts | Violations | System Events | Blocked Sources

Main | Admin | Preferences | Tasks | Log out | Help

View | Save As | Actions

Quick Filter

Basic Filter | Saved Filters

- By Severity
- By Event Type
- By Alert Type
- By Alert Number
- By Server Group
- By Service
 - Oracle (192.168.9.X)
 - MsSQL (192.168.9.X)
 - Db2 (192.168.9.X)
 - Http (192.168.9.X)
 - MySql (192.168.9.X)
- By Application
- By Share Group
- By User Name
- By Source IP
- By URL
- By Session ID
- By Remedy Incident ID
- By Violated Item
- By Violation Description
- By Gateway
- Generated by ThreatRadar
- By File Folder
- By File Parent Path
- By File Name
- By File Extension

Apply | Save | Clear | Advanced

Violations (filtered)

Time | ID | Type | Source IP | Username | Dest. IP | Violation Description

sql (30)

Time	ID	Type	Source IP	Username	Dest. IP	Violation Description
19:55:34	...7872		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7873		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7869		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7866		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7863		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7867		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7875		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7864		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7868		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:34	...7871		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7856		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7851		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7854		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7853		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7858		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7861		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7852		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7862		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7857		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7850		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7859		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7855		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:33	...7860		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7843		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7848		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7846		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7844		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7847		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7845		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin
19:55:31	...7849		192.168.10.227	db2admin	192.168.9.9	Excessive Attempts of Database Login by db2admin

Details

Event 6775268904659847872: Excessive Attempts of Database Login

Violation Type	sql
Severity	High
Policy Name	SQL Correlation Poli
Alert Number	81
Violation Description	Excessive Attempts
Violated Item	User: db2admin
Immediate Action	None
Number of Login Attempts	35
Allowed Number of Attempts	5

Event Details:

Event Time: August 23, 2011 7:55:34 PM

Server Group	Service	Application
192.168.9.X	Db2	Default

Connection	User	DB
192.168.10.227:43284 → 192.168.9.9:50000	db2admin	db2ev

Affected Rows: 0 | Response Size: 0 Records

Error Code: 0 | Error Message:

Databases and Schemas:

Database	Schemas
jpk	Scher, db2ad

Privileged Operations & Stored Procedures:

Operation	Objects
No data found	

Table Groups:

Table Group Name	Black List
No data found	

Source Application Details:

Application Name	db2jccawt-ev
Application User	
Web Session ID	None
Source URL	N/A
Web Client IP	N/A
Web Event ID	N/A

IMPERVA SECURESPHERE | Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar

Dashboard | Alerts | Violations | System Events | Blocked Sources

Main | Admin | Preferences | Tasks | Log out | Help

View | Save As | Actions

Quick Filter

Basic Filter | Saved Filters

- By Severity
- By Event Type
- By Alert Type
- By Alert Number
- By Server Group
- By Service
 - Oracle (192.168.9.X)
 - MsSQL (192.168.9.X)
 - Db2 (192.168.9.X)
 - Http (192.168.9.X)
 - MySql (192.168.9.X)
- By Application
- By Share Group
- By User Name
- By Source IP
- By URL
- By Session ID
- By Remedy Incident ID
- By Violated Item
- By Violation Description
- By Gateway
- Generated by ThreatRadar
- By File Folder
- By File Parent Path
- By File Name
- By File Extension

Apply | Save | Clear

Advanced

Violations (filtered)

Time	ID	Type	Source IP	Username	Dest. IP	Violation Description	Server Group	Violated
8/22/11 ...4375	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4373	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4362	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4356	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4354	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4321	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4185	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4183	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4173	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4167	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA
8/22/11 ...4165	1	Info	192.168.10.77	n/a	192.168.9.9	Untraceable Database User	192.168.9.X	NA

Event 378484028635874356: Untraceable Database User

Details

Untraceable Database User

Event 378484028635874356: Untraceable Database User

Key	Value
Violation Type	sql
Severity	Informative
Policy Name	SQL Profile
Alert Number	57
Violation Description	Untraceabl
Violated Item	NA
Immediate Action	None

Event Details:

Event Time
August 22, 2011 7:17:55 PM

Server Group	Service	Application
192.168.9.X	MySql	Default

Connection	User (Raw User)
192.168.10.77:62829 → 192.168.9.9:3306	connected user (user)

Affected Rows	Response Size
0	Records

Error Code	Error Message

Databases and Schemas:

Database	Schema

Privileged Operations & Stored Procedures:

Operation	Objects
No data found	

Table Groups:

Table Group Name	Black List
No data found	

Source Application Details:

Application Name

Application User

Web Session ID

Source URL

Web Client IP

Web Event ID

Additional Info:

Normalized Query

Query Group:

IMPERVA SECURESPHERE | Main | Admin | Preferences | Tasks | Log out | Help

Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar

Dashboard | Alerts | Violations | System Events | Blocked Sources

View | Save As | Actions

Quick Filter

Basic Filter | Saved Filters

- By Severity
- By Event Type
- By Alert Type
- By Alert Number
- By Server Group
- By Service
 - Oracle (192.168.9.X)
 - MySQL (192.168.9.X)
 - Db2 (192.168.9.X)
 - Http (192.168.9.X)
 - MySql (192.168.9.X)
- By Application
- By Share Group
- By User Name
- By User Name
- By Source IP
- By URL
- By Session ID
- By Remedy Incident ID
- By Violated Item
- By Violation Description
- By Gateway
- Generated by ThreatRadar
- By File Folder
- By File Parent Path
- By File Name
- By File Extension

Apply | Save | Clear | Advanced

Violations (filtered)

Time | ID | Type | Source IP | Username | Dest. IP | Violation Description

Filter: http (50)

Time	ID	Type	Source IP	Username	Dest. IP	Violation Description
19:58:25	...7962		192.168.10.227		192.168.9.9	Suspicious Response Code
19:58:25	...7963		192.168.10.227		192.168.9.9	Suspicious Response Code
8/22/11	...4783		192.168.10.77		192.168.9.9	Suspicious Response Code
8/22/11	...4781		192.168.10.77		192.168.9.9	Suspicious Response Code
8/22/11	...4774		192.168.10.77		192.168.9.9	Suspicious Response Code
8/22/11	...4766		192.168.10.77		192.168.9.9	Malformed HTTP Header Line 3
8/22/11	...4766		192.168.10.77		192.168.9.9	Abnormally Long Header Line request header name
8/22/11	...4766		192.168.10.77		192.168.9.9	Malformed HTTP Header Line 2
8/22/11	...4766		192.168.10.77		192.168.9.9	NULL Character in Header Name at [[#5]][[#0]][[#0]]
8/22/11	...4766		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Method [[#2]][[#0]][[#0]]
8/22/11	...4771		192.168.10.77		192.168.9.9	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]
8/22/11	...4771		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Header Name
8/22/11	...4771		192.168.10.77		192.168.9.9	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]A[
8/22/11	...4771		192.168.10.77		192.168.9.9	Malformed URL
8/22/11	...4771		192.168.10.77		192.168.9.9	NULL Character in Header Name at
8/22/11	...4771		192.168.10.77		192.168.9.9	Abnormally Long Request method
8/22/11	...4771		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]#
8/22/11	...4767		192.168.10.77		192.168.9.9	Unknown HTTP Request Method [[#18]][[#1]][[#0]][[#0]]4[
8/22/11	...4767		192.168.10.77		192.168.9.9	Malformed URL
8/22/11	...4767		192.168.10.77		192.168.9.9	Abnormally Long Request method
8/22/11	...4767		192.168.10.77		192.168.9.9	NULL Character in Method [[#18]][[#1]][[#0]]4[[#0]][#
8/22/11	...4767		192.168.10.77		192.168.9.9	NULL Character in Header Name at
8/22/11	...4767		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Method [[#18]][[#1]][[#0]]#
8/22/11	...4769		192.168.10.77		192.168.9.9	Abnormally Long Request method
8/22/11	...4769		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Method
8/22/11	...4769		192.168.10.77		192.168.9.9	NULL Character in Method
8/22/11	...4765		192.168.10.77		192.168.9.9	Abnormally Long Request request version
8/22/11	...4765		192.168.10.77		192.168.9.9	Unknown HTTP Request Method sqlxec in URL inf
8/22/11	...4765		192.168.10.77		192.168.9.9	Malformed URL in formix
8/22/11	...4766		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Header Name [[#1]][[#0]]#
8/22/11	...4766		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Header Name [[#5]][[#0]]#
8/22/11	...4766		192.168.10.77		192.168.9.9	Abnormally Long Header Line request header name
8/22/11	...4766		192.168.10.77		192.168.9.9	Malformed HTTP Header Line 4
8/22/11	...4766		192.168.10.77		192.168.9.9	NULL Character in Method [[#2]][[#0]][[#2]][[#0]][[#0]]
8/22/11	...4766		192.168.10.77		192.168.9.9	NULL Character in Header Name at [[#1]][[#1]][[#0]]
8/22/11	...4766		192.168.10.77		192.168.9.9	Malformed HTTP Header Line 1
8/22/11	...4766		192.168.10.77		192.168.9.9	Abnormally Long Request method
8/22/11	...4766		192.168.10.77		192.168.9.9	NULL Character in Header Name at
8/22/11	...4766		192.168.10.77		192.168.9.9	Illegal Byte Code Character in Header Name [[#1]][[#1]][[#0]]#

Event 6775268904659847962: Custom Rule Violation

Details | Response

Custom Rule Violation

Event 6775268904659847962: Custom Rule Violation !

Key	Value
Violation Type	http
Severity	Medium
Policy Name	Suspicious Response Code
Alert Number	82
Violation Description	Suspicious Response Code
Violated Item	Custom Violation
Immediate Action	None
Matched Patterns	

Event Details:

Event Time: August 23, 2011 7:58:25 PM

Server Group	Service	Application
192.168.9.X	Http	Default Web

Host	Connection
192.168.9.9	192.168.10.227:43520 → 192.168.9.9:80

User	Session
	N/A

Response Code	Response Size
400	39 Bytes

GET / HTTP/1.1
 Host 192.168.9.9:8080
 Connection: keep-alive
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/13.0.782.112 Safari/535.1
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
 Accept-Encoding: gzip,deflate,sdch
 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
 Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.3

Parameters:

File Name	Value
No data found	

Cookies:

File Name	Value
No data found	

Enrichment Data:

User Defined Field	Value
No data found	

IMPVERA SECURESPHERE

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Dashboard Alerts Violations System Events Blocked Sources

Main Admin Preferences Tasks Log out Help

View Save As Actions

Alert 2004: Excessive Attempts of Database Login by jpk

Actions: None
Policy: SQL Correlation Policy

Aggregated from 00:00:30 (0 hour(s), 10 minute(s)), 1194 alerts (last updated 00:09:34)...

Alert aggregated by:

Distinct value for:	Value	Key	Value
OS User		OS Hosts	1
Server Group	192.168.9.X	Source Applications	1
Server IP	192.168.9.9	SQL Users	4
Source IP	192.168.10.227	Tables	0

Statistical Information:

Key	Value
OS Hosts	1
Source Applications	1
SQL Users	4
Tables	0

Violations:

User	Attempt Number	Error
jpk	33	

SQL Users Distribution

User	Count
intruder	714
admin	105
root	150
jpk	225

Alerts (filtered)

No.	Updated	#	Alert Description
Last Hour (2)			
2001	01:23:40	24	Multiple violations from 192.168.9.9
2005	00:25:15	3	Suspicious Response Code
Last 2 Hours (2)			
2003	00:16:36	5	Multiple violations from 192.168.9.9
2004	00:09:34	1194	Excessive Attempts of Database Login by jpk
Yesterday (19)			
2002	8/23/11	2	Unauthorized Access to Service netbios-dgr
87	8/23/11	1	Unauthorized Access to Service microsoft-t
86	8/23/11	4	Unauthorized Access to Service netbios-dgr
80	8/23/11	100	Multiple violations from 192.168.9.9
85	8/23/11	2	Unauthorized Access to Service dns on port
84	8/23/11	2	Unauthorized Access to Service microsoft-t
83	8/23/11	2	Multiple violations from 192.168.9.9
82	8/23/11	2	Suspicious Response Code
81	8/23/11	119	Excessive Attempts of Database Login by db2adm
79	8/23/11	24	Distributed Unauthorized Access to Service: port l
78	8/23/11	47	Multiple violations from 192.168.9.9
76	8/23/11	33	Distributed Unauthorized Access to Service:
77	8/23/11	4	Unauthorized
75	8/23/11	28	Multiple vio
71	8/23/11	42	Distributed Un
73	8/23/11	48	Multiple violat
72	8/23/11	214	Multiple violat
74	8/23/11	2	Unauthorized
55	8/23/11	562	Multiple violat
Aug 22, 2011 (21)			
70	8/22/11	1	Unauthorize
53	8/22/11	129	Distributed
56	8/22/11	288	Multiple vio
69	8/22/11	2	Unauthorize
68	8/22/11	6	Suspicious R
62	8/22/11	12	Multiple Ille
61	8/22/11	36	Multiple Ille
59	8/22/11	24	Multiple Un
65	8/22/11	6	Multiple Abno
60	8/22/11	30	Multiple Abno
63	8/22/11	6	Multiple Ma
58	8/22/11	24	Multiple Malfo
64	8/22/11	18	Multiple NU
66	8/22/11	36	Multiple NU
67	8/22/11	2	Unauthorize
57	8/22/11	11	Untraceable I
54	8/22/11	2	Multiple vio
52	8/22/11	38	Multiple vio
51	8/22/11	17	Distributed
50	8/22/11	41	Multiple vio
49	8/22/11	38	Distributed
Aug 21, 2011 (6)			
48	8/21/11	17	Multiple violations from 192.168.9.9
47	8/21/11	41	Distributed Unauthorized Access to Service:
46	8/21/11	30	Multiple violations from 192.168.9.9

Apply Save Clear

Advanced

https://192.168.10.77:8083/SecureSphere/ui/main.html#

User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

IMPVERA SECURESPHERE

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Dashboard Alerts Violations System Events Blocked Sources

Main Admin Preferences Tasks Log out Help

View Save As Actions

Alert 2004: Excessive Attempts of Database Login by jpk

Actions: None
Policy: SQL Correlation Policy

Aggregated from 00:00:30 (0 hour(s), 10 minute(s)), 1194 alerts (last updated 00:09:34)...

Alert aggregated by:

Distinct value for:	Value	Key	Value
OS User		OS Hosts	1
Server Group	192.168.9.X	Source Applications	1
Server IP	192.168.9.9	SQL Users	4
Source IP	192.168.10.227	Tables	0

Statistical Information:

Key	Value
OS Hosts	1
Source Applications	1
SQL Users	4
Tables	0

Violations:

User	Attempt Number	Error
jpk	33	

SQL Users Distribution

Close

Alerts (filtered)

No.	Updated	#	Alert Description
Last Hour (2)			
2001	01:23:40	24	Multiple violations from 192.168.9.9
2005	00:25:15	3	Suspicious Response Code
Last 2 Hours (2)			
2003	00:16:36	5	Multiple violations from 192.168.9.9
2004	00:09:34	1194	Excessive Attempts of Database Login by jpk
Yesterday (19)			
2002	8/23/11	2	Unauthorized Access to Service netbios-dgr
87	8/23/11	1	Unauthorized Access to Service microsoft-t
86	8/23/11	4	Unauthorized Access to Service netbios-dgr
80	8/23/11	100	Multiple violations from 192.168.9.9
85	8/23/11	2	Unauthorized Access to Service dns on port
84	8/23/11	2	Unauthorized Access to Service microsoft-t
83	8/23/11	2	Multiple violations from 192.168.9.9
82	8/23/11	2	Suspicious Response Code
81	8/23/11	119	Excessive Attempts of Database Login by db2adm
79	8/23/11	24	Distributed Unauthorized Access to Service: port l
78	8/23/11	47	Multiple violations from 192.168.9.9
76	8/23/11	33	Distributed Unauthorized Access to Service:
77	8/23/11	4	Unauthorized
75	8/23/11	28	Multiple vio
71	8/23/11	42	Distributed Un
73	8/23/11	48	Multiple violat
72	8/23/11	214	Multiple violat
74	8/23/11	2	Unauthorized
55	8/23/11	562	Multiple violat
Aug 22, 2011 (21)			
70	8/22/11	1	Unauthorize
53	8/22/11	129	Distributed
56	8/22/11	288	Multiple vio
69	8/22/11	2	Unauthorize
68	8/22/11	6	Suspicious R
62	8/22/11	12	Multiple Ille
61	8/22/11	36	Multiple Ille
59	8/22/11	24	Multiple Un
65	8/22/11	6	Multiple Abno
60	8/22/11	30	Multiple Abno
63	8/22/11	6	Multiple Ma
58	8/22/11	24	Multiple Malfo
64	8/22/11	18	Multiple NU
66	8/22/11	36	Multiple NU
67	8/22/11	2	Unauthorize
57	8/22/11	11	Untraceable I
54	8/22/11	2	Multiple vio
52	8/22/11	38	Multiple vio
51	8/22/11	17	Distributed
50	8/22/11	41	Multiple vio
49	8/22/11	38	Distributed
Aug 21, 2011 (6)			
48	8/21/11	17	Multiple violations from 192.168.9.9
47	8/21/11	41	Distributed Unauthorized Access to Service:
46	8/21/11	30	Multiple violations from 192.168.9.9

Quick Filter

Basic Filter Saved Filters

- By Severity
- By Immediate Action
- By Alert Type
- By Alert Flag
- By Alert Number
- By Server Group
- By Service
 - MySQL (192.168.9.X)
 - Http (192.168.9.X)
 - Oracle (192.168.9.X)
 - Db2 (192.168.9.X)
 - MsSQL (192.168.9.X)
- By Application
- By Share Group
- By User Name
- By Source IP
- By URL
- By Session ID
- By Event ID
- By Remedy Incident ID
- By Gateway
- Generated by ThreatRadar
- By File Folder
- By File Parent Path
- By File Name
- By File Extension

Apply Save Clear Advanced

https://192.168.10.77:8083/SecureSphere/ui/main.html#

User: admin | Version: 8.0.0.8265.Release.Enterprise.Edition | © 2010 Imperva Inc.

Затем мы плавно перешли к тестированию связей Web приложений, здесь более всего применялся режим автоматизированного сканирования и отслеживалась активность как в мониторе на сервере управления Imperva так и на целевых хостах, посредством мониторинга логов тестируемых служб

Web сервера даже не заметили необычной активности, кроме увеличения количества hits, а пользователи ftp пытающиеся выполнить запрещённые команды после внесения пары настроек более до сервера достигать не могли, всякие «игры» с SELECT в контексте PHP никаких результатов не принесли

Так же при внедрении не следует забывать о оптимальной, на наш взгляд службе – радар угроз, который позволяет в реальном времени получать информацию и своевременно блокировать трафик «чёрных» ip адресов глобальной сети, узлов TOP, анонимных прокси-серверов, узлов замеченных в фишинге и ip адресов с подозрительной активностью



©IMPERVA SECURESPHERE Main Admin Preferences Tasks Log out Help

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Dashboard Activate Save As Actions

THREATRADAR ! Can't reach ThreatRadar servers EMERGENCY LICENSE ACTIVATION Buy > Request a Trial > Learn More >

Service	Enabled	License Expiration	License Type
All Services			
Malicious IPs	Yes		
IP Forensics	Yes		
Phishing URLs	Yes		
TOR IPs	Yes		
Anonymous Proxies	Yes		

i All services in this section are currently unlicensed. If one of the services was licensed before, the data received from ThreatRadar in the past is kept by SecureSphere. Select the service to view its details.

[Show License](#)

Alert

! Can't reach ThreatRadar servers. It seems like the Management server cannot access www.imperva.com over https. Please consult your network administrator.

OK

Main > ThreatRadar > Dashboard User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

IMPVERA SECURESHERE

Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | Threat Radar

Dashboard | Alerts | Violations | System Events | Blocked Sources

Main | Admin | Preferences | Tasks | Log out | Help

View | Save As | Actions

Quick Filter

Alerts (filtered)

Alert 2001: Multiple violations from 192.168.9.9

Actions: Immediate Block
Policy: Firewall Policy

Aggregated from 8/23/11 (3 hour(s), 37 minute(s)), 31 alerts (last updated 02:22:47)...

Alert aggregated by: Statistical Information:

Policy Details

Policy name: Firewall Policy

Policy Rules | Apply To (Read Only)

Inbound:

Block

Protocol	Source
bgp	Any
chargen	Any
citrix	Any
compaq-diag	Any
cpq-wbem	Any
cvspsserver	Any
daytime	Any
dhcp-client	Any
dhcp-server	Any
discard	Any
dns	Any
dns-zone-transfers	Any
echo	Any
finger	Any
font-service	Any
ftp	Any
fw1-secureremote	Any
gopher	Any
http	Any
http-alt	Any

Outbound:

Block

Protocol	Destination
bgp	Any
chargen	Any
citrix	Any
compaq-diag	Any
cpq-wbem	Any
cvspsserver	Any
daytime	Any
dhcp-client	Any
dhcp-server	Any
discard	Any
dns	Any
dns-zone-transfers	Any
echo	Any
finger	Any
font-service	Any
ftp	Any
fw1-secureremote	Any
gopher	Any
http	Any
http-alt	Any

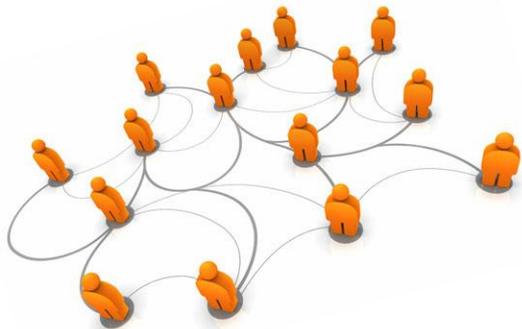
Main > Monitor > Alerts

User: admin | Version: 8.0.0.8265 Release Enterprise Edition | © 2010 Imperva Inc.

Чутьочку забегаая вперед хотим обратить ваше внимание на возможность выполнения аудита не только для собственных специалистов, но и для аттестации по требуемому уровню, например – выполнив полстью ваш аудит в системе вы сразу можете сопоставить насколько он соответствует требованиям того или иного стандарта, список стандартов на следующем слайде в виде скриншота интерфейса тестируемой системы

Далее мы рассмотрим возможности системы по пунктам, связывая их с тестами и заостряя внимание на ключевых моментах

Учитывая тот факт, что политики, мы применяли, фактически были политикам по умолчанию, то потенциал системы на самом деле намного больше чем на удалось показать в данной презентации



The screenshot displays the IMPERVA SECURESHERE Risk Management interface. The top navigation bar includes links for Main, Admin, Preferences, Tasks, Log out, and Help. Below this, a secondary navigation bar lists various modules: Risk Console, DB Assessment Policies, Custom Assessment Tests, Web Scanner Integration, Discovery & Classification, Setup, Profile, Risk Management (selected), Policies, Audit, Reports, Monitor, and ThreatRadar. On the right side of this bar are buttons for Activate, Save As, and Actions.

The main interface is divided into several sections:

- Scope Selection:** Contains links for Risk Management, Vulnerability Management, and Assessment Results.
- Views:** A list of views including Assessment Results, Summary View, Comparison View (selected), and Results Analysis. Under Results Analysis, there are several sub-items: Servers Success Rate, Tests Success Rate, Common Test Error Messages, Database Server Connectivity Errors, OS Connectivity Errors, Common OS connectivity Errors, and Common Database Connectivity Errors.
- Comparison View:** The main content area, titled "Comparison View", with a filter: "Result is [Failed] and Asset is [Service: Default Site...1] and Last Scan in Eac...". It contains the "Policy & Scan Specifications" section, which instructs the user to "Choose the policy and scan that you would like to compare their executions." Below this instruction are four selection fields:
 - Select Policy:** A dropdown menu currently showing "CIS - Security Configuration Benchmark For MySQL 5.0".
 - Select Scan:** A dropdown menu currently showing "Missing Security Patches for Oracle".
 - Select Baseline Scan Run:** A dropdown menu currently showing "Missing Security Patches for Oracle".
 - Select Target Scan Run:** A dropdown menu currently showing "Missing Security Patches for Oracle".

The bottom status bar shows the navigation path "Main > Risk Management > Risk Console", the user "User: admin", the version "Version: 8.0.0.8265.Release.Enterprise Edition", and the copyright "© 2010 Imperva Inc."

The screenshot displays the IMPERVA SECURESPHERE Risk Management interface. The top navigation bar includes links for Main, Admin, Preferences, Tasks, Log out, and Help. Below this, a secondary navigation bar lists Discovery & Classification, Setup, Profile, Risk Management (selected), Policies, Audit, Reports, Monitor, and ThreatRadar. The main content area is titled 'Risk Details' and 'Choose Data Type Risk Level View'. A search bar is located in the top right of the main area. The central part of the screen features a grid of 16 green icons, each representing a different data type: Payment Card, Phone, Amount, Payment Card PIN, Drug Name, National ID, Bank Identifier Code, Person Name, Password, National Drug Code, Email Address, Payment Card Magnetic..., Address, Account Number, Payment Card CVV, and ZIP Code. The bottom status bar shows 'Showing all 16 items' and a small laptop icon. The footer contains the breadcrumb 'Main > Risk Management > Risk Console', the user 'User: admin', the version 'Version: 8.0.0.8265.Release.Enterprise Edition', and the copyright '© 2010 Imperva Inc.'

IMPVERA
SECURESPHERE

Main Admin Preferences Tasks Log out Help

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Risk Console DB Assessment Policies Custom Assessment Tests Web Scanner Integration

Activate Save As Actions

Scope Selection

Risk Management

Vulnerability Management

Assessment Results

Filter

Views

Risk Explorer

Summary

Risk Details

Choose Data Type

Choose Data Type Risk Level View

Search

Up Filter

Network View

Data View

Payment Card

Phone

Amount

Payment Card PIN

Drug Name

National ID

Bank Identifier Code

Person Name

Password

National Drug Code

Email Address

Payment Card Magnetic ...

Address

Account Number

Payment Card CVV

ZIP Code

Showing all 16 items

Main > Risk Management > Risk Console

User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

The screenshot displays the IMPERVA SECURESPHERE Risk Management console. The main window shows the 'Risk Details' for IP 192.168.9.9, specifically the 'Risk Level View'. The interface features a navigation menu on the left with options like 'Risk Management', 'Vulnerability Management', and 'Assessment Results'. The main content area displays five green risk level indicators for different services: Oracle, MySQL, MsSQL, Http, and Db2. A legend in the bottom left corner defines the risk levels: High (red), Medium (orange), and Low (green). The status bar at the bottom indicates 'Showing all 5 items'.

Navigation: Main > Risk Management > Risk Console

User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

© IMPERVA SECURESPHERE | Main | Admin | Preferences | Tasks | Log out | Help

Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar

Risk Console | DB Assessment Policies | Custom Assessment Tests | Web Scanner Integration

Activate | Save As | Actions

Scope Selection

Risk Management
Vulnerability Management
Assessment Results

Views

Risk Explorer
Summary

Risk Details

Risk data is updated to 8/23/11 5:00:00 AM

Sites - Risk scoring and trends

Site Name	Risk Score	Daily Trend
Default Site	0	No change

Distribution Graphs

Services at Risk Breakdown by Risk level and Location

Services at Risk Breakdown by Risk level and Operating System

Services at Risk Breakdown by Risk level and Database Type

Data Types - Risk scoring and protection coverage

Data Type	Risk Level	Number Of Services	% protected
Payment Card PIN	Low (0)	0	0.0 %
Payment Card	Low (0)	0	0.0 %
Account Number	Low (0)	0	0.0 %
Payment Card Magnetic Stripe Information	Low (0)	0	0.0 %
Person Name	Low (0)	0	0.0 %
Address	Low (0)	0	0.0 %
Email Address	Low (0)	0	0.0 %
National ID	Low (0)	0	0.0 %
Drug Name	Low (0)	0	0.0 %
Payment Card CVV	Low (0)	0	0.0 %
Account	Low (0)	0	0.0 %

Main > Risk Management > Risk Console

User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

IMPVERA SECURESPHERE

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Main Admin Preferences Tasks Log out Help

View Results | Manage Reports

Activate Save As Actions

Report: Daily Report for Outbound Credit Card Numbers Visibility - Data Leakage

General Details Data Scope Tabular Data Analysis Views Scheduling

Quick Filter

Basic Filter Saved Filters

ADC Keywords

User Defined Keywords

Data Source

Alerts

DB Audit

File Audit

System Events

Tasks

Risk

Active Modules

User Rights

File User Rights Overview

Configuration

Vulnerabilities

Assessment

Profile

Discovery

Active Module Type

Defined By

Run Date

Scheduling

Apply Save Clear

Reports

Show Favorites Show Enabled

Type	Name
Type: Alerts (11)	
Alerts	Daily Report for Outbound Credit Card Numbers Visibility - Data Leakage
Alerts	Daily Report for Outbound U.S Social Security Number Visibility - Data Leakage
Alerts	Daily Summary Blocked Connections
Alerts	Daily Top 10 All Violations
Alerts	Daily Top 10 DB Violations
Alerts	Daily Top 10 WAF Violations
Alerts	List Of Alerts
Alerts	Weekly Data Leakage Summary Report
Alerts	Weekly Summary Top 10 All Violations
Alerts	Weekly Summary Top 10 DB Violations
Alerts	Weekly Summary Top 10 WAF Violations
Type: Pre-Defined Assessment (6)	
Pre-Defined Assessment	DBA Accounts
Pre-Defined Assessment	Dormant DBA Accounts
Pre-Defined Assessment	HIPAA - Password management
Pre-Defined Assessment	Non DBA accounts with admin privileges
Pre-Defined Assessment	PCI-DSS Compliance
Pre-Defined Assessment	Privileges of the DBA Role
Type: User Rights (3)	
User Rights	Unapproved Permissions Grants and Resulting Rights
User Rights	Unapproved Role Grants and Resulting Rights
User Rights	Unused Effective Rights (over a Month)
Type: DB Audit (30)	
DB Audit	Daily audit trail (Application)
DB Audit	Database configuration changes (CSV)
DB Audit	EBS - Report Data Change Activity in Financial Tables by Default Users
DB Audit	EBS - Report Data Change Activity in Foundation Tables by Default Users
DB Audit	EBS PCI - Daily access to card number (CSV)
DB Audit	EBS PCI - Daily access to cardholder (CSV)
DB Audit	EBS PCI - Weekly access to card number (CSV)
DB Audit	EBS PCI - Weekly access to cardholder (CSV)
DB Audit	HIPAA - Access management activity
DB Audit	HIPAA - Daily PHI access log (CSV)
DB Audit	HIPAA - Detailed connection log
DB Audit	HIPAA - Failed PHI access attempts
DB Audit	HIPAA - Failed connection attempts
DB Audit	HIPAA - Weekly access summary to PHI
DB Audit	PCI - Access to DB by unknown Web application users (CSV)
DB Audit	PCI - Daily access to cardholder information (CSV)
DB Audit	PCI - Failed login attempts (CSV)
DB Audit	PCI - Failed users and privileges management operations (CSV)
DB Audit	PCI - Login and Logout actions (CSV)
DB Audit	PCI - Modification of system-level objects (CSV)
DB Audit	PCI - Newly created objects under system schema (CSV)
DB Audit	PCI - Users and privileges management operations (CSV)
DB Audit	PCI - Weekly access to cardholder information (CSV)
DB Audit	PeopleSoft - Report Access to Identification Information
DB Audit	PeopleSoft - Report Access to Payment Card Information
DB Audit	PeopleSoft - Report Access to Personal Information
DB Audit	PeopleSoft - Report Changes in Login Tables

General Information

Name: Daily Report for Outbound Credit Card Numbers Visibility - Data Leakage

Description: Display Report of last 24 hours for outbound Credit Card Numbers visibility - data leakage. Supports ISO 27001 12.2.4, ISO 27001 12.5.4 and privacy regulations.

Data Type: Alerts

Followed Action:

Enable Report

Save Result on Run Now

Report Format

Format: CSV PDF

Page Orientation: Landscape Portrait

Cover Page:

Keywords

ADC Keywords: Privacy, ISO 27001

User Defined Keywords:

Report Keywords:

Run Report Now

100%

Download Report (182 KB)

Close

Main > Reports > Manage Reports

User: admin | Version: 8.0.0.8265 Release Enterprise Edition | © 2010 Imperva Inc.

Сгенерированный отчёт доступен в формате pdf

IMPVERA SECURESPHERE

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Security | Audit | Data Enrichment | System Events | Action Sets

Main Admin Preferences Tasks Log out Help

Activate Save As Actions

Audit Policy Filters

- All
 - By ADC Keywords
 - SAP
 - PCI
 - HIPAA
 - PeopleSoft
 - EBS
 - SOX
 - ISO 27001
 - Privacy
 - GLBA
 - Basel II
 - By Type
 - File Audit Application
 - DB Audit Application
 - DB Audit Service
 - By Server Group
 - 192.168.9.X
 - By Service
 - Db2 (192.168.9.X)
 - Http (192.168.9.X)
 - MySQL (192.168.9.X)
 - MySql (192.168.9.X)
 - Oracle (192.168.9.X)
 - By Application
 - Default DB2 Application (D)
 - Default MySQL Application
 - Default MySQL Application
 - Default Oracle Application
 - Default Web Application (H)
 - By Share Group

Audit Policies

Policy	Type	Update
<input type="checkbox"/> DB Audit Service		
DDL commands	DB Audit Service	7/6/11
Database configuration changes	DB Audit Service	7/6/11
Database connections	DB Audit Service	7/6/11
Default Rule - All Events	DB Audit Service	8/22/11
HIPAA - Access to PHI	DB Audit Service	7/6/11
New Databases	DB Audit Service	7/6/11
New Users Account	DB Audit Service	7/6/11
PCI - Access to cardholder information	DB Audit Service	7/6/11
PCI - Audit of newly created objects under system schema	DB Audit Service	7/6/11
PCI - Login and logout audit	DB Audit Service	7/6/11
PCI - Login audit	DB Audit Service	7/6/11
PCI - Modification audit of system-level objects	DB Audit Service	7/6/11
PCI - Privileged operations on users and privileges management	DB Audit Service	7/6/11
PCI - Unknown Web application user audit	DB Audit Service	7/6/11
Privilege Operations	DB Audit Service	7/6/11
Privilege manipulation	DB Audit Service	7/6/11
SOX - Changes to Financial Data	DB Audit Service	7/6/11
SOX - Database code changes	DB Audit Service	7/6/11
SOX - Database configuration changes	DB Audit Service	7/6/11
SOX - Database object changes	DB Audit Service	7/6/11
SOX - New objects	DB Audit Service	7/6/11
SOX - New users	DB Audit Service	7/6/11
SOX - Privilege changes over financial data	DB Audit Service	7/6/11
SOX - Table related commands	DB Audit Service	7/6/11
SOX - Users and Privileges Management Commands	DB Audit Service	7/6/11
Table related commands	DB Audit Service	7/6/11
Users and Privileges Management Commands	DB Audit Service	7/6/11
<input type="checkbox"/> File Audit Application		
Default File Audit Rule - All Events	File Audit Application	7/6/11

Policy: DDL commands

Match Criteria Apply to Settings Archiving External Logger

Policy Configuration: Command Groups is at least one of [General Object Ma...] Full

Match Criteria

- Command Groups

Available Match Criteria

- Affected Rows
- Application User
- Authentication Result
- Columns
- Command Groups
- Data Set: Attribute Lookup
- Data Type
- Database User Groups
- Database User Names
- Database and Schema
- Destination Tables
- Enrichment Data
- Event Type
- Generic Dictionary Search
- Lookup Data Set Search
- OS Host Names
- OS User Names
- Occurrence
- Operations
- Originated in Agent
- Originated in Log Collectors
- Privileged Operation
- Proxy IP Addresses
- Query Response Size
- Query Response Time
- SQL Exception Strings
- SQL Exceptions
- Sensitive Data Access
- Sensitive Dictionary Search
- Signatures
- Source Applications
- Source IP Addresses
- Source URL
- Stored Procedure
- Subject (User) of Privileged Operation
- Table Groups
- Ticket Assigned
- Time of Day
- Unanalyzed Objects

Main > Policies > Audit

User: admin | Version: 8.0.0.8265 Release Enterprise Edition | © 2010 Imperva Inc.

Можно собрать политику соответствующую требуемому стандарту

© IMPERVA SECURESPHERE Main Admin Preferences Tasks Log out Help

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

Sites Applications Global Objects Signatures Gateways Agents Settings Active Modules

Activate Save As Actions

Views

- Summary
- Workbench
- Status Analysis
 - General Status
 - Load Analysis
 - Network Activity
 - Inactive Agents
- Life Cycle
 - New Agents
 - New Data Interfaces
 - Agent Configuration Types
- Distribution in the Environment
 - Agent Versions
 - Database Servers
 - Database Types
 - Services And Server Groups
 - Gateways

Agents

Filter: Empty

Agent Name	Status	Platform	Data Interface IP	Host Name	Operating System	Gateway	Agent Version	Data Interface Service Types	Last Packet	Throughput (KB)
JPK9		x86	192.168.9.9	security-note	Microsoft Windows XP Professional	impervact	8.5.0.1022	None	Never	0

Agent Name: JPK9 Save

General Details Settings Data Interfaces Permissions Activity Log

General Information

Name	Data Interface IP	Creation Time	Manual Settings Activation
JPK9	192.168.9.9	8/23/11 11:44:52 PM	Off

Last 24 Hours: CPU Usage (%) Statistics CSV

Gateways

Gateway	Active	Data Interface IP	Port	Encrypted	Data Protocol
impervact	Yes	192.168.10.77	443 (449)	Yes	TCP

Status

General Status	Start Time	Active Gateway	Last Status Update
	8/23/11 11:46:25 PM	impervact	8/24/11 12:21:37 AM

Configuration Status Last Update Time

Configured	8/24/11 12:19:48 AM
------------	---------------------

Last Packet	Throughput (KB)	Connections Per Sec.	Hits Per Sec.	CPU%
Never	0	0	0	0

Properties

Kernel Patch	Service Pack 3 (build 2600)
Hostname	security-note
Platform	x86
Agent Version	8.5.0.1022
Operating System	Microsoft Windows XP Professional

Main > Setup > Agents User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

Можно выбрать интересующую вас информацию от агента

```
System log: created: 23/08/2011 15:46:22
```

```
Version: 8.5.0.1022
```

```
Up Time: 23/08/2011 15:46:22
```

```
Log # 1
```

```
23/08/2011 15:46:22[info]ImpervaCli.cpp:82 Starting ImpervaCli init
23/08/2011 15:46:22[info]ImpervaCli.cpp:212 Starting target directory init
23/08/2011 15:46:22[info]ImpervaCli.cpp:286 Starting collection table init
23/08/2011 15:46:22[info]ImpervaCli.cpp:324 Collection table init ended successfully
23/08/2011 15:46:22[info]ImpervaCli.cpp:337 Starting types table init
23/08/2011 15:46:22[info]ImpervaCli.cpp:376 Types table init ended successfully
23/08/2011 15:46:22[info]ImpervaCli.cpp:389 Starting types table init
23/08/2011 15:46:22[info]ImpervaCli.cpp:150 ImpervaCli init ended successfully
23/08/2011 15:46:26[info]ragentCli.cpp:639 backup of bootstrap.xml was saved in bootstrap.xml.backup22
23/08/2011 15:46:47[NOTIFICATION]PcapProxy.cpp:63 Using WinPcap version 4.1.2
23/08/2011 15:46:50[debug]TapConnection.cpp:161 Attempt to connect to 192.168.10.77:443
23/08/2011 15:46:50[debug]TapConnection.cpp:252 Client connected to socket: 188
23/08/2011 15:46:51[debug]SslConnection.cpp:736 SSL socket connect: 188 (192.168.9.9:1384->192.168.10.77:443)
23/08/2011 15:46:51[debug]SslConnection.cpp:424 SSL socket disconnect socket188 (192.168.9.9:1384->192.168.10.77:443)
23/08/2011 15:46:51[debug]TapConnection.cpp:105 closing socket: 188 (192.168.9.9:1384->192.168.10.77:443)
23/08/2011 15:46:51[debug]TapConnection.cpp:161 Attempt to connect to 192.168.10.77:443
23/08/2011 15:46:51[debug]TapConnection.cpp:252 Client connected to socket: 188
23/08/2011 15:46:51[debug]SslConnection.cpp:736 SSL socket connect: 188 (192.168.9.9:1385->192.168.10.77:443)
23/08/2011 15:46:51[debug]SslConnection.cpp:424 SSL socket disconnect socket188 (192.168.9.9:1385->192.168.10.77:443)
23/08/2011 15:46:51[debug]TapConnection.cpp:105 closing socket: 188 (192.168.9.9:1385->192.168.10.77:443)
23/08/2011 15:46:51[ERROR]RagentReg.cpp:212 Registration failed - bad username or password.
23/08/2011 15:46:51[debug]SslConnection.cpp:420 not connected socket disconnect socket 4294967295 (192.168.9.9:1385->192.168.10.77:443)
23/08/2011 15:47:07[info]ragentCli.cpp:639 backup of bootstrap.xml was saved in bootstrap.xml.backup23
23/08/2011 15:47:33[debug]TapConnection.cpp:161 Attempt to connect to 192.168.10.77:443
23/08/2011 15:47:33[debug]TapConnection.cpp:252 Client connected to socket: 188
23/08/2011 15:47:33[debug]SslConnection.cpp:736 SSL socket connect: 188 (192.168.9.9:1386->192.168.10.77:443)
23/08/2011 15:47:33[debug]SslConnection.cpp:424 SSL socket disconnect socket188 (192.168.9.9:1386->192.168.10.77:443)
23/08/2011 15:47:33[debug]TapConnection.cpp:105 closing socket: 188 (192.168.9.9:1386->192.168.10.77:443)
23/08/2011 15:47:33[debug]TapConnection.cpp:161 Attempt to connect to 192.168.10.77:443
23/08/2011 15:47:33[debug]TapConnection.cpp:252 Client connected to socket: 188
23/08/2011 15:47:33[debug]SslConnection.cpp:736 SSL socket connect: 188 (192.168.9.9:1387->192.168.10.77:443)
23/08/2011 15:47:33[debug]SslConnection.cpp:424 SSL socket disconnect socket188 (192.168.9.9:1387->192.168.10.77:443)
23/08/2011 15:47:33[debug]TapConnection.cpp:105 closing socket: 188 (192.168.9.9:1387->192.168.10.77:443)
23/08/2011 15:47:33[ERROR]RagentReg.cpp:212 Registration failed - bad username or password.
23/08/2011 15:47:33[debug]SslConnection.cpp:420 not connected socket disconnect socket 4294967295 (192.168.9.9:1387->192.168.10.77:443)
23/08/2011 15:47:52[info]ragentCli.cpp:639 backup of bootstrap.xml was saved in bootstrap.xml.backup24
23/08/2011 15:48:19[debug]TapConnection.cpp:161 Attempt to connect to 192.168.10.77:443
23/08/2011 15:48:19[debug]TapConnection.cpp:252 Client connected to socket: 188
23/08/2011 15:48:19[debug]SslConnection.cpp:736 SSL socket connect: 188 (192.168.9.9:1388->192.168.10.77:443)
23/08/2011 15:48:19[debug]SslConnection.cpp:424 SSL socket disconnect socket188 (192.168.9.9:1388->192.168.10.77:443)
23/08/2011 15:48:19[debug]TapConnection.cpp:105 closing socket: 188 (192.168.9.9:1388->192.168.10.77:443)
```

Можно загрузить через веб-интерфейс

IMPERVA SECURESPHERE | Main | Admin | Preferences | Tasks | Log out | Help

Discovery & Classification | Setup | Profile | Risk Management | Policies | **Audit** | Reports | Monitor | Threat Radar

DB Audit Data | File Audit Data | Audit Management Statistics | Archive Management

Activate | Save As | Actions

Scope

Policy: Default Rule - All Events (3,509 Events)

Time Frame: Please Select Custom..

Views

- Summary
- Data
- Statistics
- Server Analysis
 - Monitored Servers
 - Monitored Databases
 - DB Server Performance
- Source Analysis
 - Shared DB Users
 - DB Users
 - Source Applications
 - Source Hosts
 - OS Users
 - Source IPs
 - User Groups
 - Application Users (UUT)
 - Login Analysis
 - Performance by Source
- Data Access Patterns
 - Top Queries
 - Query Type Analysis
 - Sensitive Query Overview
 - Query Records
 - Data Modifications Analysis
- Privileged Operations
 - Privileged Query Overview
 - Table Drops/Truncates
 - Stored Procedure Changes
 - Changes to DB/Schemas
 - DCL Commands
 - DDL Commands
 - Native Auditing Changes
 - Newly Created Users
- Additional Views
 - Failed Logins
 - SQL Errors
 - Unmonitored (Encrypted) Logins
- Time Based Analysis
 - Daily
 - Day of the Week
 - Hour of the Day

Default Rule - All Events - Summary

Reported Period: 08/17/2011, 21:00- 08/22/2011, 19:00 (4 Days,22 hrs) Update

Filter: Empty

Hits	Logins	Users	Monitored Servers	Hosts
59	56	12	1	0

Hits Breakdown by Day:



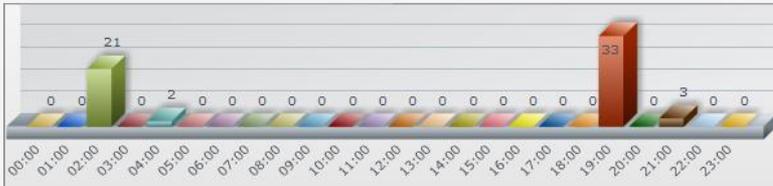
Day	Hits	Logins	Users	Monitored Servers	Hosts
August 17, 2011	3	2	1	1	0
August 19, 2011	23	23	5	1	0
August 22, 2011	33	31	11	1	0

Hits Breakdown by Day of the week:



Day	Hits	Logins	Users	Monitored Servers	Hosts
Monday	33	31	11	1	0
Wednesday	3	2	1	1	0
Friday	23	23	5	1	0

Hits Breakdown by Hour:



Hour	Hits	Logins	Users	Monitored Servers	Hosts
02:00	21	21	5	1	0
04:00	2	2	1	1	0
19:00	33	31	11	1	0
21:00	3	2	1	1	0

IMPERVA SECURESPHERE Main Admin Preferences Tasks Log out Help

Discovery & Classification Setup Profile Risk Management Policies Audit Reports Monitor ThreatRadar

DB Audit Data File Audit Data Audit Management Statistics Archive Management

Activate Save As Actions

Reports Summary Gateways Policies Management Server

Summary

Status Overview

The status of various system aspects over the last 24 hours and in the past 7 days.
The status relates to loss of audit events (actual loss or warning) due to an insufficient quota or high collection rate.

	Disk Quota	Policy Quota	Collection Rate	External Logging
Last 24 Hours	OK	OK	OK	OK
Last 7 Days	OK	OK	OK	OK

Overview

	Since System Creation	Currently collected on All Gateways
Number of Audited Events	3509	3509
Number of Logged Events (Syslog)	0	0

	Since System Creation	Currently on All Gateways
Audited Events Size	2 MB	2 MB
Responses Size	3 MB	3 MB
Index Size	436 KB	436 KB
Total	6 MB	6 MB

Top 5 Gateways by Disk Utilization (in MB)

Gateway	Free Space (MB)	Used Space (MB)
impervact	~50,000	~250,000

Top 5 Gateways by Collection Rate (Last 24 Hours Average)

Gateway	Rate (KB/sec)
impervact	~2

Top 5 Policies by Disk Utilization (in MB)

Policy	Used Space (MB)
Default...	~6
PCI - A...	~0
Privile...	~0
HIPAA - ...	~0
DDL com...	~0

Top 5 Policies by Collection Rate (Last 24 Hours Average)

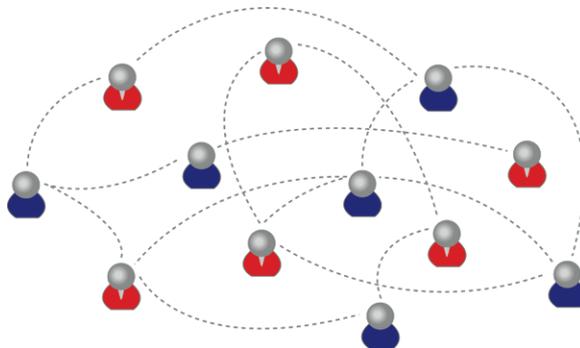
Policy	Rate (KB/Sec)
Default...	~2
SOX - N...	~0
New Dat...	~0
HIPAA - ...	~0
DDL com...	~0

Main > Audit > Audit Management Statistics

User: admin | Version: 8.0.0.8265.Release.Enterprise Edition | © 2010 Imperva Inc.

Основные аргументы в пользу данной системы:

- способна сразу после установки и настройки сетевых параметров с политиками по умолчанию «приступить» к защите вашего внутреннего периметра
- шлюз можно устанавливать в режиме прозрачного моста, что никак не повлияет на текущую конфигурацию вашей сети
- благодаря постоянным автоматическим обновлениям сигнатур и комплексу «радар угроз» вам не нужно будет беспокоиться о обновлении ваших СУБД и веб-сервисов исключительно из соображений безопасности
- благодаря встроенным средствам и политикам вы можете поддерживать свою систему в соответствии с требуемым стандартом безопасности
- вы получаете великолепную систему мониторинга и оповещения, у ваших специалистов всегда будет актуальная информация





Благодарим за внимание!