Auditing The Oracle Database

PFCATK – A Toolkit to Help
Pete Finnigan – Background, Who Am I?

• Oracle Security specialist and researcher
• CEO and founder of PeteFinnigan.com Limited in February 2003
• Writer of the longest running Oracle security blog
• Oracle ACE for security
• Member of the OakTable
• Speaker at various conferences
  – UKOUG, PSOUG, BlackHat, more..
• Published many times, see
  – http://www.petefinnigan.com for links
• Influenced industry standards
  – And governments

Sorry I cannot be there in person but we are working on something later in the year
Agenda

• Do people use Oracle audit trails?
• A bit of history
• The Focus - The PFCLATK toolkit
• An overview
• Deployment
• Hacking
• Audit results
State of the (Audit Trail) Nation

- Extensive experience visiting customer sites
  - Performing security audits
  - Reacting to incidents, breaches or attacks
- I see one common theme
  - No audit trails OR
  - Very limited audit trails OR
  - Of those that do have audit trails very few use them interactively
- Sometimes people collect audit because they have to (regulations)
- I have even seen some sites collect audit and delete it (regulations)
History of the Toolkit and Talks

• In 2009 piece of work to help design audit trails
  • Site had limited staff, little time to design, deploy, maintain any audit trails
  • I came up with some simple ideas, proof of concepts – to package up audit trails for them; inc policy based audit, IPS and simple firewall
  • They spent limited time to deploy a useful audit trail
• Similar piece of work in 2011 where limited team needed to deploy audit
• 2012 to 2015 extended the toolkit
• I wrote a presentation back in 2012 and presented it just once at a SIG on practical audit trails where I mentioned this toolkit for the first time
• This then became the basis of a one day class on the same subject
• Reworked that presentation in UKOUG 2015 conference
• Customer in 2016 needed an audit trail to deploy quickly
• Deployed now to customers in UK, Ireland and Germany
My Sample Application Architecture

- Oracle Linux
- Oracle SE1 Database
- Applications (Front Facing Website, back office customer processing)

Server 1 – Linux 5.9

Server 2 – Linux 5.9

Server 3 – Linux 5.9

Oracle database schemas

Orablog Schema

End Users

Apache / PHP / OCI8

BOF: Back Office web based Application

Apache / PHP / OCI8

Orablog: Web Based CMS Application

DBA, DEV and Application Support Users

Power Users
Demo Hacking

Demo:

• Enable secconf.sql to get standard audit
• Run audit.sql to see audit configuration
• Test some SQL Injection as an attacker
• SQL Injection attack as unauthenticated web user
• SQL Injection attack as database user with just CREATE SESSION
• Access data as a DBA with %ANY% rights
• View audit trail generated
The Goal of the Toolkit

• As simple as `SQL> @atk` and a sophisticated audit trail is up and running
• Making it simple for organisations to deploy audit trails simply, with no resources
• No design, implement, test etc as we have done it for you already
• Used in ATC mode – space also is managed in each target database audited
• Simple to configure or not configured at all
• A complete solution to know what is happening at the database engine level for sites with limited resources
PFCLATK – “A”udit “T”rail tool”K”it

• Toolkit to aid audit trail deployment easily
• Simple pre-configure
• Policy based
• Alert based
• Multiple audit trails sources
• Add in factors (input hints)
• Separated schema design
• Manual 25 pages currently
• Version 1.7.2.0 currently
• Layered audit
PFCLATK Block Overview

- Free PL/SQL and SQL based toolkit – 14k lines of code.
- Audit the database engine itself

PFCLATK is a toolkit for auditing database security. It includes features such as System Privileges, Audit Actions, Policy and Rules, and API's. The toolkit also has functionality for Escalate and Admin tasks. The Security of The Database and Audit Layers are audited through various layers including OS, Database, Security of The Audit Layer, and Audit of Audit Layers. The toolkit also includes ATK Audit Trails and ATK Alerts for monitoring and reporting.
PFCLATC – “A”udit “T”oolkit “C”entralised

- PFCLATK can be deployed to each “target Oracle Database”
- PFCLATC is an additional layer to add centralisation of those audits automatically
  - Simple configuration to link each target with the central storage
  - Uses links and a PUL mechanism
  - Audit trails are check summed
  - Audit trails are PUL’d
  - Audit trails purged from the target
- Manage target space needed for audit trails (limited by PUL)
- The toolkit also audits the PFCLATC target (if required)
- Central reporting possible over many databases
PFCLATK Architecture

- The PFCLATK toolkit is designed to be deployed to a target or central database
- When enabled simply adding target link details to the ATC database starts the PUL process automatically
Database Engine Audit

- Sites often have application level audit trails
  - In the application layer itself
  - Sometime also in the database (RLA in Oracle E-Business Suite for instance)
- Sites sometimes have audit enabled at the operating system level
- Auditing of the database is often
  - Application related
  - Regulation related
- **Audit is needed at the database engine layer to capture abuse against the database itself**
Alerts

• React in real time to attacks
  • SQL Injection
  • Privilege abuse
  • Error conditions
• React in
  • Real time where possible
  • Semi-real time if not possible
• Other reactions can be slower or not at all
• Alerts are configured in policies along with raw audit collected – post filtering is more powerful than unified audit pre-filtering because we can filter across more domains
Separated Schemas and Roles

• Schemas
  • ATKD – The owner of tables, views, sequences
  • ATK – The owner of the main API. Also runs jobs that payloads and filters based on

• Roles
  • ATK_ADMIN - Any user granted this role can set up PFCLATK rules, policies, jobs, filters, credentials and factors
  • ATK_REPORT – Any user granted this role can view the alerts and alert details and audit trail details
Configuration

-- There variables can control the operation of this install script

```sql
define DEBUG = "OFF"  -- turn debug ON or OFF, results in the O/P file
define TBLSPC = "USERS"  -- define the tablespace for ATK, must be created first
define ATC = "ON"  -- Turn on or off to install the ATC objects and code
define DROPATK = "OFF"  -- if ON call drop anyway, if OFF test if ATK is installed
  -- before dropping ATK
```

-- End of customer changeable values

The user configurable settings are simple and at the top of
atk.sql
Factors

Some factors are re-defined, some should be edited and more can be added easily

Factors allow the toolkit to be customised for a specific site
Audit Policies

```
begin
-- create the policy
atk.pfclatk.createpolicy('PROFILEPRIVILEGE');

-- audit profiles
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Create Profile','CORE-S','create profile');
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Drop Profile','CORE-S','drop profile');
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Alter Profile','CORE-S','alter profile');
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Profile','CORE-S','profile');

-- --------------------------------------------------
-- Add filter job to detect non-legitimate profile changes - i.e. use
-- of PROFILE system privileges; not use of statement PROFILE and not use
-- of a DBA IP address and not use of a DBA account; so if a DBA
-- uses a non DBA account from his own IP it should be detected
-- --------------------------------------------------

atk.pfclatk.addfilter('NON-AUTH-PROFILE-CHANGE','PROFILEPRIVILEGE','HALF HOUR',
   '[Alert] Non-legitimate profile privilege change',
   'select ''|a.action_name||'' on ''|a.obj_name||'' by

-- enable the policy
atk.pfclatk.enablepolicy('PROFILEPRIVILEGE');
end;
```

- Policies declare collection of raw data and also events
- PFCLATK policies are different to Unified audit – we filter on collected data after storage to look for abuse; Unified audit filters before storage
- Core audit, DML, System triggers
Alert Jobs

--- In this setup we create a number of database jobs that can be used
--- to attach payloads to. Each time a job runs it queries the payloads
--- table and runs all payloads that are attached to the respective job
--- frequency that is running.
---
--- We will create seven jobs (BUT more can be created as necessary)
---
--- MINUTES : 2 minutes
--- HALF HOUR : 30 minutes
--- ONE HOUR : 1 Hour (used for PUL)
--- TWO HOUR : 2 Hours (Used for PUL)
--- HALF DAY : 12 Hours
--- WEEK : 1 Week
--- MONTH : 1 Month
--- YEAR : 1 year
---
--- IMMEDIATE: immediate
---
--- There is also a job type of IMMEDIATE but this is not run as a job
--- in the database as a trigger or code elsewhere can execute these
--- job types and their payloads.
---
--- create the IMMEDIATE job. This is slightly different as it does
--- not create a DBMS_JOB job.
---
--- @@check.sql "IMMEDIATE: Create the immediate job"
---
--- declare
--- lv_job varchar2(100);
--- begin
--- create the job
--- lv_job:=atk.pfclatk.createjob('IMMEDIATE',NULL,100001);
--- start the job
--- atk.pfclatk.enablejob(lv_job);
---
--- end;
--- /
Audit of Audit

• A multi-layer approach is needed
  • Audit of core trail tables such as AUD$
  • Audit of core audit settings such as AUDIT$
  • Audit of triggers (Event, DDL and DML)
  • Audit of custom logs
  • Audit of audit functionality, packages and other objects
• All can be set up as policies in PFCLATK
Configure and Deploy

• Edit atk.sql
  • Edit required settings needed for the toolkit
• Edit conf.sql
  • Add connection details
• Demo deployment
  • Run atk.sql
Demo Hacking

Demo:
- All ATK policies are enabled
- Test some SQL Injection as an attacker
- SQL Injection attack as unauthenticated web user
- SQL Injection attack as database user with just CREATE SESSION
- Access data as a DBA with %ANY% rights
Reports

• A few sample reports exist that highlight issues
  • Audit_report.sql
  • Car.sql
• Alerts are viewed via the ATKD.PFCLATK_ALERTS table
• Alert details in ATKD.PFCLATK_ALERT_ROWS
  • tr.sql shows high level summary of alerts

Demo: look at the audit trails
Live Training in Ljubljana, Slovenia

• I am sorry that I could not be there in person today!
• If you would like to learn much more in details about audit trails in Oracle then I offer a 1 day class that we are planning to hold in November with Palsit
• The class details are here - http://www.petefinnigan.com/training/Practical_Audit_Trail_Class_Flyer.pdf
• If you are interested please speak to Palsit or myself
Conclusions

• Start to audit the database engine
• Understand what people are doing at the database engine level
• Take advantage of a simple to use idea to enable policies and factors
• Deploy with a simple command
• Close the gap between OS and application audit
• GDPR is coming and you need to detect attacks (successful or not)
Auditing The Oracle Database

PFCATK – A Toolkit to Help