PFCL

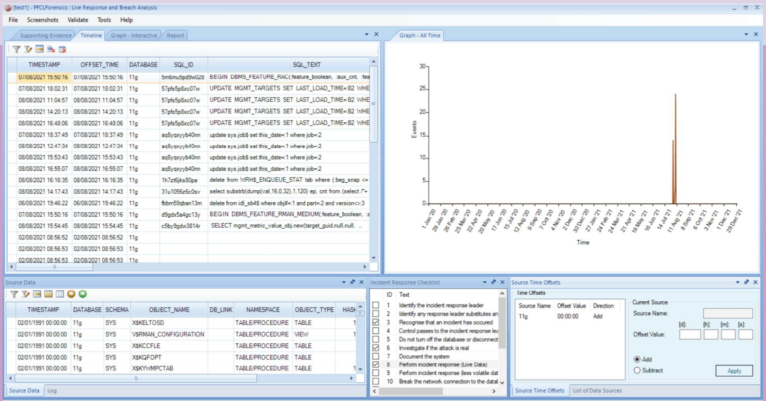
PETEFINNIGAN.COM LIMITED

PFCLForensics - Live Response and Forensics

PFCLForensics Version 3.0 is a simple to use but comprehensive tool to use to assist any organisation that has potentially been breached. The tool supports three major operations:

- A team can use its checklist feature to manage the incident resonse process from start to finish.
- Database incident response team can perform live analysis of transient artefacts and also more static data.
- An analyst can use the product to process and investigate the evidence that has been gathered.

A breach can be mangaged in terms of working through the steps needed to respond to and analyse a potential breach; PFCLForensics helps with this. The steps can be checked off as they are reached and completed. PFCLForensics can be used to provide live response on a database and also the operating system in respect to the database server.



TIMESTAMP	OFFSET_TIME	DATABASE	SQL_ID	SQL_TEXT
07/08/2021 15:50:16	07/08/2021 15:50:16	11g	5m6mu5pd9w028	BEGIN DBMS_FEATURE_RAC(:feature_boolean, :aux_cnt, :fea
07/08/2021 18:02:31	07/08/2021 18:02:31	11g	57pfs5p8xc07w	UPDATE MGMT_TARGETS SET LAST_LOAD_TIME=:B2 WHE
08/08/2021 11:04:57	08/08/2021 11:04:57	11g	57pfs5p8xc07w	UPDATE MGMT_TARGETS SET LAST_LOAD_TIME=:B2 WHE
08/08/2021 14:20:13	08/08/2021 14:20:13	11g	57pfs5p8xc07w	UPDATE MGMT_TARGETS SET LAST_LOAD_TIME=:B2 WHE
08/08/2021 16:48:06	08/08/2021 16:48:06	11g	57pfs5p8xc07w	UPDATE MGMT_TARGETS SET LAST_LOAD_TIME=:B2 WHE
07/08/2021 18:37:49	07/08/2021 18:37:49	11g	aq8yqxyyb40nn	update sys.job$ set this_date=:1 where job=:2
08/08/2021 12:47:34	08/08/2021 12:47:34	11g	aq8yqxyyb40nn	update sys.job$ set this_date=:1 where job=:2
08/08/2021 15:53:43	08/08/2021 15:53:43	11g	aq8yqxyyb40nn	update sys.job$ set this_date=:1 where job=:2
08/08/2021 16:55:07	08/08/2021 16:55:07	11g	aq8yqxyyb40nn	update sys.job$ set this_date=:1 where job=:2
08/08/2021 16:16:35	08/08/2021 16:16:35	11g	1h7zt6jks80pa	delete from WRH$_ENQUEUE_STAT tab where (:beg_snap <=
08/08/2021 14:17:43	08/08/2021 14:17:43	11g	31u1056z6c0sv	select substrb(dump(val,16,0,32),1,120) ep, cnt from (select /*+
06/08/2021 19:46:22	06/08/2021 19:46:22	11g	fbbm59qban13m	delete from idl_sb4$ where obj#=:1 and part=:2 and version<>:3
07/08/2021 15:50:16	07/08/2021 15:50:16	11g	d9gdx5a4gc13y	BEGIN DBMS_FEATURE_RMAN_MEDIUM(:feature_boolean, :a
08/08/2021 15:54:45	08/08/2021 15:54:45	11g	c5by9gdw3814r	SELECT mgmt_metric_value_obj.new(target_guid,null,null, ...
02/08/2021 08:56:52	02/08/2021 08:56:52	11g		
02/08/2021 08:56:53	02/08/2021 08:56:53	11g		
02/08/2021 08:56:53	02/08/2021 08:56:53	11g		

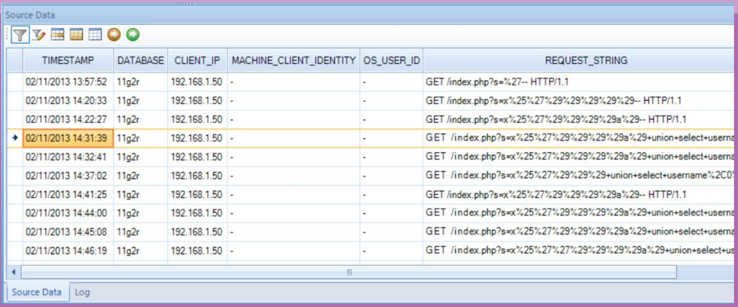
TIMESTAMP	DATABASE	SCHEMA	OBJECT_NAME	DB_LINK	NAMESPACE	OBJECT_TYPE	HASH
02/01/1991 00:00:00	11g	SYS	X$KELTOSD		TABLE/PROCEDURE	TABLE	1
02/01/1991 00:00:00	11g	SYS	V$RMAN_CONFIGURATION		TABLE/PROCEDURE	VIEW	1
02/01/1991 00:00:00	11g	SYS	X$KCCFLE		TABLE/PROCEDURE	TABLE	
02/01/1991 00:00:00	11g	SYS	X$KQFOPT		TABLE/PROCEDURE	TABLE	
02/01/1991 00:00:00	11g	SYS	X$KYWMPCTAB		TABLE/PROCEDURE	TABLE	1

	ID	Text
□	1	Identify the incident response leader
□	2	Identify any response leader substitutes an
☑	3	Recognise that an incident has occured
□	4	Control passes to the incident response lea
□	5	Do not turn off the database or disconnect
☑	6	Investigate if the attack is real
□	7	Document the system
☑	8	Perform incident response (Live Data)
□	9	Perform incident response (less volatile dat
□	10	Break the network connection to the datal

Time Offsets

Source Name	Offset Value	Direction
11g	00:00:00	Add

Current Source
Source Name:
Offset Value: [d]: [h]: [m]: [s]:
● Add
○ Subtract



TIMESTAMP	DATABASE	CLIENT_IP	MACHINE_CLIENT_IDENTITY	OS_USER_ID	REQUEST_STRING
02/11/2013 13:57:52	11g2r	192.168.1.50	-	-	GET /index.php?s=%27-- HTTP/1.1
02/11/2013 14:20:33	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29%29-- HTTP/1.1
02/11/2013 14:22:27	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29a%29-- HTTP/1.1
02/11/2013 14:31:39	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29a%29+union+select+userna
02/11/2013 14:32:41	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29a%29+union+select+userna
02/11/2013 14:37:02	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29+union+select+username%2C0
02/11/2013 14:41:25	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29a%29-- HTTP/1.1
02/11/2013 14:44:00	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29a%29+union+select+userna
02/11/2013 14:45:08	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%29%29%29%29a%29+union+select+userna
02/11/2013 14:46:19	11g2r	192.168.1.50	-	-	GET /index.php?s=x%25%27%27%29%29%29%29a%29+union+select+us

The product also supports projects so that each analysys is self contained. Each set of data gathered during the live response has a checksum created at extraction time from the database or server if done in the tool or at the time of loading the file into PFCLForensics. These checksums are verified every time the project is loaded and the user can request a validation at any time in the interface.

Request a Demo

If you would like to receive further details of this exciting product or request a demo then please email: sales@petefinnigan.com

PFCLForensics is a very powerful tool that can be used to support a breach response process and team; to perform a live response on one or many databases and servers and also files; and finally to allow forensic analysis and investigation and report writing to answer the basic questions:

- Was there an actual breach?
- How did the attacker get in?
- What rights did the attacker have?
- What data did the attacker see?
- What did the attacker change?
- What could the attacker have done with more skill?

Key Features

Project Based: to allow multiple investigations to be undertaken or practice responses.

Checksums: All of the data extracted from a database or server or from a file is checksummed to prove the data has not changed.

Sources: Load data from databases, servers and adhoc files.

File Load: pre-defined file types can be loaded but you are also able to define your own file types.

Time Sync: Because each source, database, server or file can have a slightly different time when compared to a unique wall clock.

Logs and Trace: The tool allows logging and trace to be enabled to record actions made in the tool. This can provide an audit trail of actions.

List Data Sources: All data sources gathered for all systems in a project visible in one list so that individual data can be viewed in details.

Timeline: Build a time line of only relevant evidence.

Supporting Data: Other imporant data that is relevant but not actual evidence of an attack can be saved to the supporting time line.

Drillable Graph: The timeline is represented as a grid but also as a drillable timeline to home into clusters of evidence.

Overall Timeline: View all events captured as one complete timeline so that the whole expanse of the attack can be viewed as one timeline.

Filtering: Create simple or complex filters of the data in the source grids to target what evidence might be needed. The filtering is also reflected in the graphs.

Sorting: Sort any columns of data in the source data or timeline or supporting evidence grids.

Report: Fully functional word processor is built in that allows the responder to create a detailed report of the attack and to use any data in the tool as screen shots or raw data.

Licensing

Engagement License

An engagement license is aimed at a consultant who needs to perform a database security audit internally once or for a client but who does not need to use the PFCLScan + Applications software for a year or longer.

An engagement license has all the same features as a Pro annual license but the license term lasts instead for 30 days. This license is great for a single audit or a single engagement. The fee is again based on our same installation based model and does not limit the number of targets that can be scanned in one company.

This engagement license can be purchased for a single engagement to perform an audit internally or for your customers if you are a consultant. You can renew the engagement license for an 18% discount provided that the renewal is concurrent to the original license.

Pro License

This license has the same features as the engagement license but the license lasts for one year. The software can be installed on one PC only in your own company OR at one customer of yours - The implications of consultant use of the license are discussed below.

Enterprise License

This license and software is the same as the Pro license with the exception that you may install the software as many times as you need within your own company OR at one customer of yours - The implications of consultant use of the license are discussed below.

License	Seats	Targets	Term	License Fee	Renewal Fee
Pro	1	Unlimited	1 year	£1095	£585
Enterprise	Unlimited	Unlimited	1 year	£2,995	£1,755
Engagement	1	Unlimited	30 days	£145	£115

* Prices in GBP. Price does not include VAT or any other local taxes.

Postal Address:
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
YO30 4XL

Phone:
+44 (0)1904 557620

E-mail:
sales@petefinnigan.com

PFCLForensics