بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

جرم‌شناسی در پایگاه‌داده Oracle

پیشگفتار

رشد روز افزون حجم اطلاعات از یک سو و پیشرفت فن‌آوری‌های نوین از سوی دیگر سبب شده تا طیف وسیعی از تهدیدها و جرایم در پایگاه‌داد مطرح گردد. وجود این تهدیدها و جرایم سبب شده تا توجه به تمهیدات امنیتی نظیر حفظ محرمانگی، صحت و دسترس‌پذیری در این سامانه‌ها از جایگاه ویژه‌ای برخوردار باشد. مکانیزم‌های امنیتی موجود، به سبب حفظ کارایی سامانه نمی‌توانند جلوی تمامی تهدیدها و جرایم اینترنتی در پایگاه‌های داده را بگیرند و لذا امکان وقوع جرم در سامانه امکان‌پذیر است. از این‌رو، به منظور شناسایی شواهد جرم، جمع‌آوری اطلاعات مربوطه، تجزیه‌وتحلیل آن‌ها و در نهایت تهیه مستندات لازم جهت اثبات وجود جرم، شاخه‌ی جرم‌شناسی پایگاه‌داده مطرح گردید. وجود زیرساخت‌های مختلف برای سامانه‌های پایگاه‌داده، طبیعت چند بعدی سامانه‌ها، ابزارهای مختلف جرم‌شناسی و فقدان مدیریت دانش مرتبط با جرم‌شناسی را می‌توان از جمله چالش‌های اصلی در این حوزه دانست. وجود این چالش‌ها سبب شده است تا جرم‌شناسی پایگاه‌داده به عنوان یک موضوع حساس و پیچیده معرفی گردد.

در این راستا بر آن شدیم تا جرم‌شناسی در سامانه Oracle را برای برخی از عملکردهای پر کاربرد، مورد بحث و بررسی قرار دهیم. بدین منظور، با استفاده از فرآیند استاندارد جرم‌شناسی، مراحل شناسایی، گردآوری اطلاعات، تحلیل، ترمیم و ارائه مستندات کافی برای اثبات جرم را تشریح می‌کنیم. لازم به ذکر است که اگر چه جرم‌شناسی پایگاه‌داده از حدود سال ۲۰۰۴ مطرح است اما تا کنون پیشرفت خاصی در زمینه‌ی ابزارهای تجاری و رایگان برای رسیدگی به رویدادهای غیرمجاز ارائه نشده است.

در ادامه و در فصل اول، مفاهیم و تعاریف اولیه‌ی جرم‌شناسی پایگاه‌داده، چالش‌ها، اهداف و گام‌های اجرایی جرم‌شناسی تشریح می‌شود. در فصل دوم، فرآیند جرم‌شناسی و مدیریت جرم فارغ از نوع پایگاه‌داده مورد بحث و بررسی قرار می‌گیرد. در فصل‌های سوم تا ششم، گام‌های شناسایی، جمع‌آوری شواهد، استخراج و تحلیل اطلاعات، ترمیم و ارائه مستندات مربوط به جرم، به ترتیب برای هر یک از رویدادهای درج، حذف و مشاهده غیرمجاز محتوای جداول، بروزرسانی غیرمجاز محتوای جداول، تغییر غیرمجاز شمای پایگاه‌داده و تلاش برای ورود غیرمجاز به سامانه پایگاه‌داده مطالعه می‌شود. لازم به ذکر است که کلیه پیکربندی‌های ارائه شده در مستند حاضر بر Oracle Database 12c Enterprise Edition می‌باشد.

فهرست مطالب

۱ جرم شناسی پایگاه‌داده

بسیاری از سازمان‌ها و آژانس‌های دولتی از پایگاه‌داده برای ذخیره و بازیابی اطلاعات استفاده می‌کنند. از آنجاییکه داده‌های سازمان‌ها می‌توانند حاوی اطلاعات حساس و حیاتی باشند، لذا حفاظت از پایگاه‌داده به عنوان یک سامانه ذخیره‌سازی اطلاعات، یک امر حیاتی و مهم به حساب می‌آید. داده‌های ذخیره شده در پایگاه‌داده ممکن است توسط کاربران غیرمجاز (از درون سازمان یا بیرون سازمان) تغییر داده شوند. لازم به ذکر است که بسیاری از مجرمان به دلیل فقدان دلایل کافی برای اثبات جرم، محکوم نمی‌شوند. در این شرایط، جرم‌شناسی نقش مهمی در ارایه روش‌های اثبات شده علمی برای جمع‌آوری اطلاعات، تحلیل و بررسی و نهایتا ارائه‌ی شرح مفصلی از فعالیت‌های مجرمانه‌ی سایبری ایفا می‌کند. جرم‌شناسی پایگاه‌داده، شاخه‌ای از جرم‌شناسی دیجیتال است که در آن پایگاه‌داده و فراداده‌های مرتبط با آن به صورت قانونی مورد مطالعه قرار می‌گیرند. یکی از مهم‌ترین اهدفی که در جرم‌شناسی پایگاه‌داده دنبال می‌شود آن است که تشخیص دهیم چه کسی، چه زمانی، چه داده‌ای را تغییر داده است. لازم به ذکر است که پایگاه‌داده قربانی معمولاً شامل اطلاعاتی است که در طول تحقیقات قانونی به کار می‌آید. در ادامه برخی از تعاریف و مفاهیم کلیدی، چالش‌ها، اهداف و گام‌های اجرایی فرآیند جرم‌شناسی در سامانه پایگاه‌داده، مورد بحث و بررسی قرار می‌گیرد.

۱-۱ تعاریف و مفاهیم

در این بخش، برخی از مهم‌ترین تعاریف و مفاهیم جرم‌شناسی پایگاه‌داده که در سرتاسر مستند مورد استفاده قرار گرفته است، مورد بحث و بررسی قرار می‌گیرد.

سامانه مدیریت پایگاه‌داده: به نرم افزاری اطلاق می‌شود که برای نگهداری و مدیریت حجم وسیعی از اطلاعات طراحی شده و مورد استفاده قرار می‌گیرد [۴].

جرم‌شناسی: مجموعه‌ای از آزمایش‌ها یا روش‌های علمی است که در تحقیقات جنایی مورد استفاده قرار می‌گیرد. امروزه جرم‌شناسی به روشی برای به دست آوردن شواهد جنایی به منظور ارائه در دادگاه اشاره دارد.

تجزیه و تحلیل جرم‌شناسی: به فرآیند بررسی رویدادهای غیرمجاز با در نظر گرفتن خط زمانی[1] موجود از شواهد فیزیکی مربوط به آن، تجزیه و تحلیل جرم‌شناسی اطلاق می‌شود. نتایج حاصل می‌تواند در شناسایی مجرم کمک کند و همچنین به منظور ارایه شواهد برای اثبات جرم، مورد استفاده قرار گیرد [۱].

[1] Timeline

جرم‌شناسی دیجیتال: به فرآیندی که در آن از روش‌های علمی مرسوم و اثبات شده برای: (۱): حفاظت، (۲): جمع‌آوری، (۳): اعتبارسنجی، (۴): شناسایی، (۵): تجزیه‌وتحلیل، (۶): تفسیر، (۷): مستندسازی و ارائه‌ی شواهد دیجیتال به منظور تسهیل در بازسازی رویدادهای شناخته شده جنایی یا پیش‌بینی اقدامات غیرمجاز استفاده می‌شود، جرم شناسی دیجیتال اطلاق می‌گردد [۵].

جرم‌شناسی پایگاه‌داده: جرم‌شناسی پایگاه‌داده فرآیندی است که تلاش می‌کند تا زمان/چگونگی/ چرایی و عامل (های) رویداد غیرمجاز در سامانه را مشخص نماید. لازم به ذکر است که محتوای پایگاه‌داده، فراداده‌ها[۲] (به ویژه فایل‌های رویدادنگاری) و داده‌های موجود در حافظه از جمله مهمترین مولفه‌های تاثیرگذار در این فرآیند به حساب می‌آیند.

ممیزی:[۳] به نظارت و ثبت فعالیت‌های کاربران در پایگاه‌داده، ممیزی اطلاق می‌شود [۶].

رویدادنگاری:[۴] به تاریخچه‌ای از فعالیت‌های اجرا شده توسط سامانه مدیریت پایگاه‌داده اطلاق می‌شود که برای تضمین ویژگی‌های جامعیت (ACID[۵]) به هنگام خرابی سخت افزاری[۶] یا از کار افتادگی ناگهانی[۷] مورد استفاده قرار می‌گیرد [۷].

مصنوعات[۸] پایگاه‌داده: رکوردها یا اطلاعاتی هستند که از پایگاه‌داده قابل استخراج بوده و در تجزیه و تحلیل جرم‌شناسی مفید هستند [۲].

رویداد غیرمجاز: به رویدادی اطلاق می‌شود که به صورت خصمانه یا ناخواسته در روال عادی سیستم تغییر نامطلوبی را ایجاد می‌کند.

۲-۱ چالش‌ها

جرم‌شناسی پایگاه‌داده، چالش‌های زیادی به همراه دارد که آن را تبدیل به یک موضوع پیچیده می‌کند. سامانه‌های پایگاه‌داده، سرویس‌ها و زیرساخت‌های مختلفی دارند که از یک پایگاه‌داده به پایگاه‌داده دیگر، متفاوت هستند. علاوه بر این، پایگاه‌های داده مختلف دارای مصنوعات جرم‌شناسی متفاوت همچون روش‌ها، مدل‌ها، چارچوب‌ها، ابزارها، فعالیت‌ها و خط‌مشی‌های مختلف هستند از سوی دیگر، سامانه‌های پایگاه‌داده

---

[2] Metadata
[3] Auditing
[4] Logging
[5] Atomicity-Consistency-Isolation-Durability
[6] Hardware failure
[7] Crash
[8] Artifact

دارای طبیعت چند بعدی شامل سطح داخلی، سطح مفهومی و سطح خارجی هستند. سطح داخلی شامل فایل فیزیکی است و سطح مفهومی، سطح منطقی است که زیرساخت منطقی شمای پایگاه‌داده ازجمله کاربران، جداول، شاخص‌ها و رویه‌ها را نمایش می‌دهد. سطح خارجی با کاربران واقعی سروکار دارد تا بتوانند داده‌ها را تغییر دهند. بنابراین، ابعاد مختلف پایگاه‌داده در جرم‌شناسی پایگاه‌داده ایفای نقش می‌کنند [۸].

یک چالش مهم دیگر در حوزه جرم‌شناسی پایگاه‌داده، تشخیص وجود نقض[9] امنیتی در سامانه است. در واقع، فرآیند شناسایی و ترمیم به هنگام وقوع جرم، تا زمانی که شخصی فکر کند که نقض امنیتی رخ داده است، به تاخیر می‌افتد. در حالت کلی، شواهد برای وجود نقض امنیتی را می‌توان در سه دسته‌ی زیر خلاصه کرد:

- داده‌های سازمان در خارج از سازمان پیدا می‌شوند که مسلماً عادی و مجاز نیست.
- رویدادی مشاهده می‌شود که غیرمنتظره است؛ مثلاً فرآیندی در زمان اشتباه اجرا شده است یا دسترسی به سامانه، خارج از ساعت‌های اداری و مجاز اتفاق افتاده است.
- نشانه‌هایی از تغییر غیرمجاز داده‌ها وجود داشته باشد.

روش‌هایی برای جمع‌آوری و تجمیع شواهد مجرمانه در پایگاه‌داده وجود دارد. جرم‌شناسی پایگاه‌داده زمانی رخ می‌دهد که از مأمور ممیزی، نحوه وقوع نقض امنیتی و شخص مجرم، درخواست شود. روش‌هایی که برای جرم‌شناسی پایگاه‌داده وجود دارند، اصولاً دارای دو محدودیت زیر هستند:

- کاربر پس از هفته‌ها یا ماه‌ها متوجه نقض امنیتی در پایگاه‌داده می‌شود. در این صورت داده‌های ناپایدار در پایگاه‌داده به عنوان شواهد وجود ندارد.
- ممکن است هیچ ممیزی برای پایگاه‌داده فعال نباشد.

دو عامل فوق‌الذکر سبب می‌شوند که بررسی رویداد مورد تقاضا، زمان آن و نتیجه‌ی حاصل از بررسی در پیچیده‌ترین حالت ممکن قرار گیرد. آنچه جرم‌شناسی پایگاه‌داده را از جرم‌شناسی شواهد فیزیکی متمایز می‌کند، حجم پایگاه‌داده و نیاز به در حال اجرا ماندن آن در محیط عملیاتی است.

۱-۳ اهداف

برخی از مهم‌ترین اهدافی که در جرم‌شناسی پایگاه‌داده به دنبال آن هستیم به قرار زیر است [۸-۹]:

ردگیری[10] اعمال DML و DDL: در چرخه حیات پایگاه‌های داده بارها نیاز می‌شود که تغییرات در داده‌ها همچون درج، بروزرسانی و حذف داده‌ها که از اعمال دستکاری داده (DML) به حساب می‌آیند و تغییرات در

[9] Breach

اشیای پایگاه‌داده همچون ایجاد، تغییر و حذف یک جدول که از اعمال تعریف داده (DDL) به حساب می‌آیند، ردگیری و بررسی شوند. با این کار، رویدادهای غیرمجاز تشخیص داده شده و مجرمان شناسایی می‌شوند.

شناسایی داده‌ها پیش و پس از تراکنش: در طول یک تراکنش، ممکن است داده‌ها دستخوش تغییرات زیادی شوند. گاهاً داده‌های جدیدی ایجاد، داده‌های موجود حذف یا تغییر داده می‌شوند. شناسایی تغییرات اعمال شده بر روی داده‌ها، ما را در تشخیص رویدادهای غیرمجاز کمک خواهد کرد.

بازگشت به عقب اعمال غیرمجاز تغییر داده: در صورتی که داده‌ها طی رویدادهای غیرمجاز تغییر داده شوند، باید بتوان آن‌ها را به وضعیت پیش از رویداد غیرمجاز بازگرداند. همچنین در صورت حذف داده‌ها، نیاز به بازیابی داده‌های حذف شده خواهد بود.

اثبات یا رد وقوع نقض امنیتی: یک چالش مهم در حوزه جرم‌شناسی پایگاه‌داده، تشخیص وجود نقض امنیتی در سامانه است. در واقع فرآیند شناسایی و ترمیم به هنگام وقوع جرم، تا زمان تشخیص نقض امنیتی در سامانه به تاخیر می‌افتد. پس از آن با طی کردن گام‌های مطرح در فرآیند جرم‌شناسی پایگاه‌داده می‌توان ثابت کرد که نقض امنیتی رخ داده است یا خیر.

تعیین محدوده‌ی نفوذ به پایگاه‌داده: هنگامی که به پایگاه‌داده حمله می‌شود، تشخیص حمله‌ی انجام گرفته و محدوده‌ی نفوذ به منظور شناسایی خسارات وارد شده و محدوده‌ی تغییرات غیرمجاز، از اهمیت بالایی برخودار است.

کشف اینکه چه اتفاقی در چه زمانی رخ داده است: با بررسی و تحلیل رویدادهای ثبت شده، اطلاعاتی همچون کاربر اجراکننده رویداد، زمان رخداد، داده متاثر از رویداد، چگونگی تغییر و علت آن مشخص می‌شود. با دانستن این اطلاعات، نه تنها جزییات رویدادهای رخ داده مشخص می‌شوند بلکه می‌توان با توجه به توالی زمانی رویدادها و تجمیع آن‌ها، اطلاعات جدیدی نیز کسب کرد. برخی از داده‌ها به تنهایی دارای ارزش کمی هستند ولی هنگامی که با سایر اطلاعات ترکیب می‌شوند، می‌توانند نقض امنیتی را آشکارتر سازند.

---

[1] Trace

۱-۴ گام‌های اجرایی

گام‌هایی که برای جرم‌شناسی پایگاه‌داده باید برداشته شوند به موقعیت و نوع سامانه مدیریت پایگاه‌داده‌ی وابسته است. در ادامه، برخی از مهم‌ترین گام‌هایی که در این راستا می‌بایست لحاظ شود، آورده شده است.

۱. **مرحله‌ی شناسایی:** در مرحله‌ی شناسایی، رویداد و نوع آن با توجه به نشانه‌های موجود در سامانه شناسایی می‌شود. این مرحله از آن جهت مهم است که سایر مراحل را تحت تأثیر قرار می‌دهد. برخی از مهمترین اهدف این مرحله، شناسایی مفاهیم مرتبط با بررسی جرم‌شناسی همچون منابع پایگاه‌داده، منابع سیستم‌عامل، منابع شبکه، تیم‌های بررسی، روش‌های بررسی، محیط بررسی، خط‌مشی‌ها، قوانین و مجوزها هستند.

۲. **تعیین روش جمع‌آوری داده‌های جرم‌شناسی:** به منظور بررسی پایگاه‌داده آسیب‌دیده یا مورد سوءاستفاده، سه روش جمع‌آوری داده به شرح زیر وجود دارد:

- **جمع‌آوری داده‌ها به صورت زنده**[1]: این روش جمع‌آوری داده زمانی اتفاق می‌افتد که سامانه مورد تجزیه و تحلیل به طور همزمان در حال سرویس‌دهی نیز می‌باشد.
- **جمع‌آوری داده‌ها به صورت غیرزنده**[2]: روش جمع‌آوری داده به صورت غیرزنده، شامل نسخه‌برداری داده‌ها از سیستم مورد بررسی است.
- **جمع‌آوری داده‌ها به صورت ترکیبی**[3]: روش جمع‌آوری داده‌ها به صورت ترکیبی با بهره‌گیری از ویژگی‌های کلیدی هر دو روش قبل، ترکیبی از این دو روش را برای جمع‌آوری داده در پیش می‌گیرد.

لازم به ذکر است که صرف‌نظر از روش مورد استفاده می‌بایست این اطمینان حاصل شود که شواهد دیجیتالی حفظ و نگهداری می‌شوند و داده‌ها به صورت ناخواسته تغییر نمی‌کنند یا از بین نمی‌روند.

۳. **جمع‌آوری مصنوعات ناپایدار[4] و پایدار:** مصنوعات و اطلاعات مختلف را می‌توان از پایگاه‌داده، سیستم‌عامل، سرورهای وب یا فایل‌های رویدادنگاری استخراج کرد. لازم به ذکر است که جمع‌آوری مصنوعات و شواهد در سامانه می‌تواند سبب تغییر در پایگاه‌داده شود. از این‌رو، پیش از استخراج اطلاعات از پایگاه‌داده باید نسبت به این موضوع و پایدار یا ناپایدار بودن اطلاعات، آگاهی پیدا کرد.

---

1 Live acquisition
1 Dead acquisition
1 Hybrid acquisition
1 Volatile artifacts

1
2
3
4

هر پایگاه‌داده شواهد مربوط به اعمال مختلف را در فایل‌های رویدادنگاری مختلفی پایگاه‌داده ذخیره می‌کند. این بدین معناست که برای تجزیه و تحلیل جرم‌شناسی می‌بایست نسبت به چگونگی عملکرد پایگاه‌داده، محل فایل‌ها و مصنوعات مختلف اطلاع داشت. مصنوعات در سطح پایگاه‌داده به دو دسته تقسیم می‌شوند: ۱): داده‌های فرار و ۲): داده‌های غیر فرار که در ادامه به تشریح هر یک از آنها می‌پردازیم.

- **داده‌های فرار:** به برخی از داده‌ها که به منظور افزایش سرعت، قابلیت اطمینان و بهره‌وری پایگاه‌داده درحافظه‌های ناپایدار ذخیره می‌شوند، داده‌های فرار اطلاق می‌شود. به عنوان نمونه، پایگاه‌داده اوراکل اطلاعات زیادی را در SGA[۸] به منظور افزایش کارایی ذخیره می‌کند. لازم به ذکر است که به طور معمول این دسته از داده‌ها دائما و با سرعت بالایی در حال تغییر هستند.
- **داده‌های غیرفرار:** به رکوردهای ذخیره شده در پایگاه‌داده، داده‌های غیرفرار یا پایدار اطلاق می‌شود.

ذکر این نکته ضروری است که فرآیند جرم‌شناسی در سامانه پایگاه‌داده نباید تنها بر روی پایگاه‌داده متمرکز باشد. پایگاه‌داده در یک محیط مجزا در حال اجرا و سرویس‌دهی نیست و متکی به زیرساخت مهمی چون سیستم عامل است. بنابراین باید سایر مصنوعات و اطلاعات جانبی از سیستم عامل‌ها و رویدادهای ثبت شده در سرور را نیز جمع‌آوری و آنها را بررسی نمود.

۴. **حفاظت[۶] و احراز اصالت[۷] داده‌های جمع‌آوری شده:** هدف از این مرحله آن است که مقدار شواهدی که مجدداً بر روی آن‌ها اطلاعاتی نوشته می‌شود، کاهش پیدا کند. مراقبت‌های شدیدی برای تضمین عدم تغییر غیرمنتظره داده‌ها باید انجام شود. اگر چه داده‌ها را می‌توان با ارسال پرسمان به پایگاه‌داده‌ی تغییریافته به دست آورد، باید از اجرای هر نوع پرسمانی که باعث حذف اطلاعات از پایگاه‌داده شود، اجتناب نمود. علاوه بر این، در صورت وجود پایگاه‌داده آسیب‌دیده یا مورد سوء استفاده قرار گرفته، صرف‌نظر از روش بدست آوردن داده، هیچ عبارت SQL ای نباید اجرا شود؛ زیرا باعث تغییر داده‌های ذخیره‌شده در حافظه و صفحات داده مربوط به پایگاه‌داده می‌شود. این کار همچنین باعث تقسیم شدن صفحه داده داخلی و محل ذخیره‌سازی داده‌های جدید در

[۸] قسمتی از حافظه‌ی سیستم که میان تمامی پردازه‌های مربوط به یک نمونه‌ی واحد از پایگاه‌داده‌ی اوراکل مشترک است.

[6] Preservation
[7] Authentication

حافظه پنهان[۱۸] می‌شود و فرآیند بررسی را پیچیده‌تر می‌کند. بنابراین باید پیش از فرآیند جمع‌آوری، نسخه پشتیبان از داده‌ها و فایل‌های مهم تهیه گردد. لازم به ذکر است که روش‌ها و ابزارهای مورد استفاده برای جمع‌آوری اطلاعات و شواهد می‌بایست تا حد امکان قابل اطمینان باشند.

۵. **تجزیه و تحلیل شواهد و تعیین فعالیت‌های مهاجم:** تجزیه و تحلیل داده‌های جمع‌آوری شده به نوع داده‌ها، سامانه پایگاه‌داده و رویداد خاصی که قرار است مورد بررسی قرار گیرد، بستگی دارد. مرحله‌ی تجزیه و تحلیل می‌بایست ابعاد مربوط به هر رویداد و محلی که اطلاعات مربوطه یافت می‌شود را در نظر بگیرد. بنابراین در مرحله‌ی تجزیه و تحلیل، اطلاعاتی همچون شخص مجرم، زمان ارتکاب جرم، داده هدف، دلایل ارتکاب و نحوه اجرای جرم تعیین می‌گردد. تجمیع داده‌ها در فرآیند جرم‌شناسی پایگاه‌داده از اهمیت بسزایی برخوردار است. برخی از داده‌ها به تنهایی دارای ارزش کمی هستند اما هنگامی که با سایر اطلاعات ترکیب می‌شوند، می‌توانند نقض امنیتی را آشکارتر سازند.

۶. **بازسازی پایگاه‌داده:** در بررسی پایگاه‌داده آسیب‌دیده یا مورد سوءاستفاده، داده‌هایی که قبلاً حذف شده‌اند، باید بازیابی و اقدامات انجام شده توسط مهاجم شناسایی شوند.

۷. **ارائه مستندات:** در مرحله آخر، کلیه‌ی بررسی‌های صورت گرفته در یک قالب استاندارد مستند و به مدیر سامانه و دادگاه ارائه می‌شود. لازم به ذکر است که مستندات تهیه شده برای سایر بررسی‌کنندگان که سناریوی مشابه‌ای را تجربه می‌کنند و همچنین برای حفاظت از پیگردهای قانونی بررسی‌کنندگان در آینده مفید خواهد بود.

۱-۵ جمع‌بندی

در این فصل به طور مشروح به معرفی مفاهیم جرم‌شناسی پایگاه‌داده و همچنین بررسی چالش‌ها، اهداف و گام‌های اجرایی در فرآیند جرم‌شناسی پایگاه‌داده پرداخته شد. در این راستا و در ابتدا، وجود تنوع‌های گسترده از سامانه‌ها، سطوح مختلف داخلی، مفهومی و خارجی پایگاه‌داده و نحوه تشخیص وقوع جرم به عنوان مهم‌ترین چالش مطرح در حوزه جرم‌شناسی پایگاه‌داده بررسی گردید. در ادامه، برخی از مهم‌ترین اهداف جرم‌شناسی پایگاه‌داده، تحت عناوینی چون شناسایی و اثبات وقوع جرم، کشف رویداد غیرمجاز و زمان وقوع آن، تعیین محدوده نفوذ و بازگرداندن وضعیت سامانه به وضعیت قبل از وقوع جرم معرفی گردید. در نهایت نیز، گام‌های اجرایی فرآیند جرم‌شناسی پایگاه‌داده از مرحله شناسایی جرم تا ارائه مستندات مربوط به شواهد وقوع جرم، تشریح گردید.

---

[1] Cache [8]

۲ شناسایی و مدیریت جرم

پژوهش‌های انجام شده در زمینه‌ی جرم‌شناسی دیجیتال منجر به توسعه‌ی روش‌ها و مدل‌های فرآیندی مختلفی شده است. بسیاری از این روش‌ها به سبب ویژگی‌های خاص هر یک از سامانه‌های پایگاه‌داده، به طور کامل قابل انطباق با جرم‌شناسی پایگاه‌داده نبوده و می‌بایست در آن‌ها تغییراتی صورت پذیرد. با استفاده از مدل‌های فرآیند جرم‌شناسی پایگاه‌داده می‌توان به صورت ساختاریافته، عملیات مربوط به جرم‌شناسی پایگاه‌داده را پیش برد. در این فصل، ابتدا تمهیدات مورد نیاز برای فراهم کردن بستر مناسب برای جرم‌شناسی در پایگاه‌داده مورد مطالعه قرار می‌گیرد. در ادامه و در بخش دوم نیز به شرح و بررسی فرآیند جرم‌شناسی در سامانه پایگاه‌داده می‌پردازیم. در بخش پایانی نیز ملاحظات و رهنمون‌های مورد نیاز برای رهگیری و انجام مراحل موجود در فرآیند جرم‌شناسی تشریح می‌گردد.

۲-۱ تمهیدات جرم‌شناسی

در این بخش، تمهیدات لازم برای جرم‌شناسی پایگاه‌داده را در طیف وسیعی از نیازمندی‌ها از پیش از وقوع جرم تا نیازمندی‌های نهایی مربوط به ارائه مستندات و اثبات وقوع جرم، مورد بحث و بررسی قرار می‌دهیم. لازم به ذکر است که داشتن طرح و برنامه دقیق، مهمترین گام در فرآیند جرم‌شناسی است. در یک دسته‌بندی کلی می‌توان تمهیدات مورد نیاز برای فرآیند جرم‌شناسی پایگاه‌داده را در موارد زیر خلاصه کرد [۱۵-۱۷]:

۱. **تعیین مدیر فرآیند:** این تمهید پیش از وقوع جرم انجام می‌شود. پیش از آنکه جرمی رخ دهد، شخصی باید به عنوان هماهنگ‌کننده تعیین شود. این شخص باید فرآیند تجزیه و تحلیل جرم‌شناسی را رهبری کند و از مستند تهیه شده از فرآیند به عنوان یک چک لیست[۱] برای اطمینان از اجرای گام به گام فرآیند استفاده نماید. علاوه بر این می‌بایست تیمی تحت رهبری هماهنگ‌کننده نیز وجود داشته باشد که از مهارت‌های امنیتی و مدیریتی در حوزه پایگاه‌داده برخوردار باشند. همچنین وجود یک مجموعه از ابزارها برای استفاده در فرآیند تجزیه و تحلیل بسیار مهم است. هریک از ابزارها و هر آنچه که هر ابزار انجام می‌دهد، می‌بایست مستند شود. بزرگترین چالش در فرآیند تجزیه و تحلیل، عدم وجود ابزارهای استاندارد رایگان به منظور تجزیه و تحلیل فایل‌های ردیابی[۲] و رویدادهای تولید شده توسط پایگاه‌داده است. در صورتی که در طول فرآیند جرم‌شناسی از ابزاری استفاده شود، باید بتوان ثابت کرد که ابزارهای مورد استفاده، شواهد جمع‌آوری

[1] Checklist
[2] Trace files

شده را تغییر نمی‌دهند و حذف نمی‌کنند. در صورتی که ابزار توسط خود افراد ایجاد شده باشد، اثبات عدم تغییر در شواهد، می‌تواند دشوار باشد. بنابراین بهتر است از ابزارهای تجاری از پیش تعیین شده‌ای که در دادگاه‌ها قابل قبول و استناد هستند، استفاده شود. لازم به ذکر است که ابزارهای مورد استفاده نیز می‌بایست از حیث امنیتی قابل اعتماد باشند و اجازه ندهند مهاجم از طریق آن‌ها به شواهد موجود خدشه‌ای وارد کند.

۲. **تعیین مولفه مرکزی برای اطلاع‌رسانی:** تعیین مولفه‌ی مرکزی برای گزارش جرم‌های حادث شده به عنوان یک تمهید پیش از وقوع جرم، از اهمیت بالایی برخوردار است. وجود این مولفه سبب می‌شود تا ذینفعان به سرعت از وقوع نقض امنیتی مطلع و بررسی آن را در دستور کار خود قرار دهند.

۳. **تشخیص وقوع نقض امنیتی:** به محض تشخیص نقض امنیتی در سامانه می‌بایست اطلاعات کافی برای مولفه مرکزی ارسال گردد. مولفه مرکزی نیز اطلاع‌رسانی‌های لازم را در این رابطه برای سایر ذینفعان ارسال می‌کند.

۴. **انتقال کنترل فرآیند به مدیر هماهنگ‌کننده:** به محض تشخیص وقوع نقض امنیتی در سامانه و اعلام آن توسط مولفه مرکزی، کنترل فرآیند به مدیر تجزیه و تحلیل جرم‌شناسی منتقل می‌شود تا این اطمینان حاصل شود که فرآیند به درستی و با دقت توسط تیم دنبال می‌شود.

۵. **پرهیز از قطع اتصال شبکه و خاموش کردن سامانه:** در این گام، به هیچ وجه نباید سامانه پایگاه‌داده خاموش یا اتصال آن به شبکه قطع گردد. توجه به این نکته حائز اهمیت است که داده‌ها و شواهد ناپایدار با خاموش شدن سیستم از بین می‌روند. اینکه مهاجم از ادامه‌ی فعالیت‌های مخرب باز بماند، ایده‌ی خوبی است ولی از دست دادن شواهد ناپایدار، بررسی‌های آتی را ممکن است با مشکل روبرو کند.

۶. **بررسی واقعی بودن حمله:** در این مرحله می‌بایست وجود نقض امنیتی و حمله به سامانه بررسی گردد. لازم به ذکر است که بررسی در دسترس بودن داده‌های حساس به طور ویژه برای مهاجم و در حالت کلی در بستر عمومی وب از اهمیت بالایی در این مرحله برخوردار است.

۷. **جمع‌آوری داده‌های فرار:** در این گام، رسیدگی به نقض امنیتی را آغاز نموده و داده‌های فرار را از روی سرور پایگاه‌داده جمع‌آوری می‌نماییم. از جمله داده‌های فرار می‌توان به اطلاعات مربوط به کاربران وارد شده به سامانه، پردازه‌های در حال اجرا، پورت‌های و فایل‌های باز، اشاره کرد. همچنین تمامی فایل‌های رویدادنگاری پایگاه‌داده، فایل‌های ردیابی و فایل‌های پیکربندی نیز باید جمع‌آوری و از آن‌ها به درستی نسخه‌برداری شود. علاوه بر این، از رویدادهای ثبت شده توسط سرور وب و برنامه‌ی کاربردی و سایر فایل‌های رویدادنگاری مهم نیز باید نسخه‌ای تهیه شود. اطلاعات موجود در حافظه نیز باید تخلیه و ثبت شوند. به عنوان نمونه، در پایگاه‌داده اوراکل اطلاعات موجود در SGA باید تخلیه و ثبت شوند. می‌توان آخرین پرسمان SQL اجرا شده را از SGA به دست آورد. در

صورتی که بررسی جرم‌شناسی خیلی سریع انجام شود، شانس این وجود دارد که عبارت‌های SQL که قسمتی از حمله بوده‌اند، در SGA وجود داشته باشند. همچنین می‌توان نشست‌ها و پردازه‌های موجود در SGA را نیز استخراج و جمع‌آوری کرد. تقریباً هرکاری که در پایگاه‌داده انجام می‌شود، آن را تغییر می‌دهد. بنابراین استخراج شواهد از پایگاه‌داده آسیب‌دیده می‌بایست با دقت و با ترتیب درستی انجام شود. لازم به ذکر است که داده‌هایی که بیشتر در معرض تغییر قرار دارند، باید سریعتر استخراج شوند.

۸. **جمع‌آوری داده‌های غیرفرار:** پس از جمع‌آوری داده‌های فرار که حساسیت بیشتری برای جمع‌آوری اطلاعات نسبت به سایر اطلاعات را دارند، سایر شواهد را نیز از پایگاه‌داده جمع‌آوری می‌کنیم. از جمله این شواهد می‌توان به لیست کاربران، مجوزهای کاربران و عضویت در نقش‌ها اشاره کرد.

۹. **قطع اتصال پایگاه‌داده به شبکه:** پس از جمع‌آوری اطلاعات و شواهد مورد نیاز برای بررسی جرم، به منظور کاهش مخاطرات احتمالی ناشی از آن می‌بایست اتصال سامانه به شبکه را قطع نمود.

۱۰. **تهیه نسخه پشتیبان:** در صورت امکان از کل دیسک سخت افزاری و یا در صورت وجود محدودیت، از شواهد موجود در سرور پایگاه‌داده، نسخه پشتیبان تهیه شود.

۱۱. **انجام تجزیه و تحلیل بر روی داده‌ها:** در این گام، بر روی داده‌ها و شواهد جمع‌آوری شده تجزیه و تحلیل صورت می‌گیرد و سعی می‌شود تا حد امکان زمان شروع و خاتمه‌ی حمله به دست آید. لازم به ذکر است که زمان‌های به دست آمده ممکن است با بررسی‌های بیشتر، تغییر نمایند.

۱۲. **ایجاد جدول زمانی[1] از رویدادها:** جدول زمانی، تمامی اطلاعات مربوط به اعمال انجام شده بر روی پایگاه‌داده را در خود جای داده است. بدین ترتیب می‌توان پی برد که:

- مهاجم چگونه به سیستم دسترسی پیدا کرده است،
- از طریق چه نام کاربری وارد شده است،
- چه اطلاعاتی را مشاهده نموده است،
- چه اعمالی را در پایگاه‌داده انجام داده است،
- با چه مجوزهایی به سیستم وارد شده است،
- و چه کارهای بیشتری را با مهارت بیشتر می‌توانست در سامانه اعمال کند.

۱۳. **خاموش کردن سیستم و بازگرداندن[2] آن به وضعیت پیش از حمله:** در این گام می‌بایست با توجه به میزان اهمیت پایگاه‌داده، برای خاموش کردن آن تصمیم‌گیری شود. پیش از خاموش کردن

[1] Timeline [2]

یا بازگرداندن پایگاه‌داده، باید کاملاً مشخص شود که مهاجم چه کارهایی را انجام داده است. در صورتی که داده‌ها تنها توسط مهاجم خوانده شده باشند و هیچ تغییری در آن‌ها اعمال نشده باشد، نیازی به بازگرداندن پایگاه‌داده به نقطه‌ای پیش از حمله نیست.

۱۴. **تهیه مستند از حمله:** مستندسازی فرآیند و کلیه‌ی شواهد جمع‌آوری شده، بسیار مهم است. همچنین باید یافته‌ها و آنچه با بررسی به دست آمده‌است نیز مستند شود. تمامی اعمال مهاجم به همراه نشانه‌هایی از سرقت داده‌ها باید ثبت شوند. ثبت اطلاعاتی همچون سیستم عامل سِرور و نسخه‌ی آن، نوع و نسخه‌ی پایگاه‌داده، رویداد غیرمجاز، نوع رویداد (خصمانه/ناخواسته)، شیوه ممیزی، منابع رویدادنگاری، شیوه یا ابزار تحلیل و امکان ترمیم در یک قالب استاندارد ضروری است. این مستندات برای شناسایی نقاط ضعف سامانه از اهمیت ویژه‌ای برخوردار است. بنابراین شناسایی نقاط ضعف سامانه و پیشنهادهایی برای حل آن‌ها نیز در این مستند ثبت می‌شوند.

۱۵. **گزارش رویدادها و فرآیند طی شده:** پس از تهیه‌ی مستند از رویدادها و فرآیند طی شده، مجموعه مستند گردآوری شده قابل ارائه به دادگاه یا سایر مقامات قانونی است.

۲-۲ فرآیند جرم‌شناسی

با استفاده از مدل‌های فرآیند جرم‌شناسی پایگاه‌داده می‌توان به صورت ساختاریافته‌ای عملیات مربوط به جرم‌شناسی پایگاه‌داده را پیش برد. در ابتدا و پیش از انجام هر عملی، باید نسبت به وقوع رویداد غیرمجاز اطمینان حاصل کرد و آن رویداد را شناسایی نمود. به عنوان مثال، در صورتی که مدیر پایگاه‌داده نسبت به حذف برخی از نام‌های کاربری از پایگاه‌داده مطلع شود، فرآیند جرم‌شناسی برای یافتن اطلاعاتی پیرامون این رویداد و ترمیم داده‌های حذف شده، آغاز می‌گردد.

پس از شناسایی وقوع رویداد غیرمجاز می‌بایست شواهد و اطلاعات پیرامون رویداد، جمع‌آوری گردد. با توجه به اینکه پایگاه‌داده در یک محیط مجزا نبوده و با سیستم عامل و برنامه‌های کاربردی در ارتباط است، می‌توان شواهد را از منابع مختلف به دست آورد. در جمع‌آوری اطلاعات و شواهد توجه به این نکته حائز اهمیت است که برخی از اطلاعات همچون داده‌های موجود در حافظه، فرار بوده و هر لحظه احتمال از دست رفتن آن‌ها وجود دارد؛ بنابراین، اینگونه از اطلاعات باید هرچه سریعتر و پیش از فرا رسیدن موعد حذف، جمع‌آوری شوند. پس از آن، می‌توان اطلاعات پایدار و غیرفرار را استخراج و در مکانی امن نگهداری کرد.

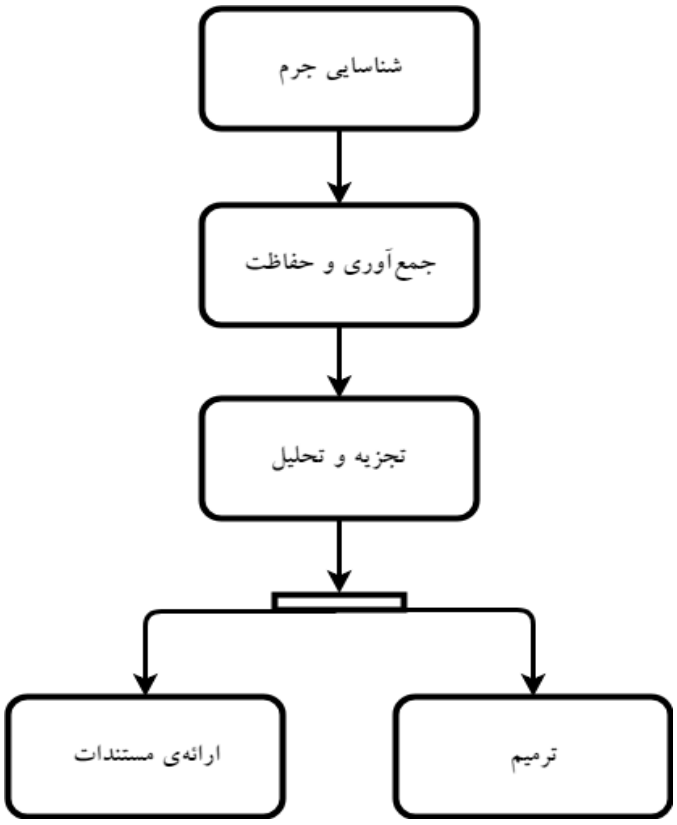
---

[2] Restore [2]

اطلاعات و شواهد جمع‌آوری شده در صورتی برای تجزیه و تحلیل و همچنین ارائه در دادگاه‌های قانونی قابل قبول هستند که به درستی حفاظت شده باشند و بتوان ثابت کرد که در حین فرآیند جرم‌شناسی تغییری در آنها صورت نگرفته است.

در ادامه و در مرحله‌ی تجزیه‌وتحلیل، با بررسی و تحلیل داده‌های جمع‌آوری شده، اطلاعاتی همچون چه‌کسی تغییر را ایجاد کرده، چه‌زمانی تغییر رخ داده، چه داده‌ای تغییر داده شده، چرا و چگونه تغییر رخ داده است، مشخص می‌شود. لازم به ذکر است که تجمیع داده‌ها در فرآیند جرم‌شناسی پایگاه‌داده از اهمیت بالایی برخوردار است. برخی از داده‌ها به تنهایی دارای ارزش کمی هستند ولی هنگامی که با سایر اطلاعات ترکیب می‌شوند، می‌توانند نقض امنیتی را آشکار سازند. تمامی شواهد جمع‌آوری شده و فرآیند طی شده در جرم‌شناسی می‌بایست مستند شود. مستندات و گزارش‌های تهیه شده قابل ارائه به مدیریت سازمان و دادگاه در صورت نیاز خواهند بود.

به سبب گستردگی حوزه جرم‌شناسی پایگاه‌داده، تمرکز ما در فرآیند جرم‌شناسی پایگاه‌داده تنها بر روی اطلاعات ثبت‌شده در پایگاه‌های داده می‌باشد و استفاده از اطلاعات ثبت‌شده بر روی سیستم عامل، داده‌های موجود در حافظه و شبکه نادیده گرفته شده است. لازم به ذکر است که برای داشتن طرحی جامع در این زمینه، در نظر گرفتن کلیه مولفه‌های درگیر ضروری است. شکل ۱، گام‌های فرآیند جرم‌شناسی پایگاه‌داده در رویکرد اتخاذی را به تصویر کشیده است. در ادامه، هر یک از این گام‌ها مورد بحث و بررسی قرار گرفته است.



شکل ۱: فرآیند پیشنهادی جرم‌شناسی پایگاه‌داده منطبق با فرآیند استاندارد

شناسایی جرم:

فرآیند جرم‌شناسی با مشاهده رویدادهای غیرمجاز در سامانه آغاز می‌شود. منظور از رویدادهای غیرمجاز، رویدادهای خصمانه یا ناخواسته‌ای هستند که مدیر پایگاه‌داده انتظار وقوع آن‌ها را در شرایط فعلی ندارد. به عنوان مثال، در صورتی که مدیر پایگاه‌داده کاربرانی را در جدولی از پایگاه‌داده تعریف کرده باشد، درج کاربر جدیدی که توسط مدیر انجام نشده است، یک رویداد غیرمجاز به شمار می‌آید.

برخی از رویدادهای قابل بررسی در فرآیند جرم‌شناسی در سامانه مدیریت پایگاه‌داده عبارتند از:

- **درج، حذف و مشاهده‌ی غیرمجاز محتوای جداول:** رویدادهای غیرمجازی هستند که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شوند و موجب درج سطر (های) جدید، حذف سطر (های) موجود یا مشاهده تمامی یا بخشی از جدول (ها) در پایگاه‌داده می‌گردند. سه رویداد فوق، از جمله دستورات دستکاری داده (DML)[۲۳] در پایگاه‌داده به حساب می‌آیند.
- **بروزرسانی غیرمجاز داده‌های جداول**: رویداد غیرمجازی است که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شود و سبب تغییر سطر (های) موجود می‌گردد. این رویداد نیز از جمله دستورات DML در پایگاه‌داده است. لازم به ذکر است که به سبب اهمیت بروزرسانی داده‌ها و چالش‌هایی که برای شناسایی وقوع جرم وجود دارد، این رویداد در برخی از سمپادها از دیگر رویدادهای مربوط به دستورات دستکاری داده متمایز شده است.
- **تغییر غیرمجاز شمای پایگاه‌داده:** رویداد غیرمجازی است که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شود و سبب تغییر شمای جدول (ها) در پایگاه‌داده می‌گردد. این رویداد توسط دستورات تعریف داده (DDL)[۲۴] در پایگاه‌داده قابل اعمال است.
- **تلاش برای ورود غیرمجاز به پایگاه‌داده:** رویداد غیرمجازی است که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شود و به طور معمول دو هدف زیر را دنبال می‌کند:
  - حدس نام کاربری و کلمه عبور کاربران مجاز جهت ورود به سامانه.

---

2 Data Manipulation Language 3
2 Data Definition Language 4

- تلاش برای شناسایی شناسه یکتای سامانه[۵](SID) و نهایتا دسترسی به حساب‌های کاربری و اعمال نفوذ در سامانه.

لازم به ذکر است که در برخی سمپادها، این تلاش تنها از طریق حدس نام‌کاربری و کلمه عبور کاربران مجاز جهت ورود به سمپاد امکان‌پذیر است.

- **تغییر غیرمجاز در فایل‌های رویدادنگاری و ممیزی:** رویداد غیرمجازی است که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شود و هدف آن از بین بردن فایل‌های رویدانگاری به منظور پاک کردن شواهد رویدادهای مجرمانه در پایگاه‌داده است.

جمع‌آوری اطلاعات و شواهد:

مصنوعات و اطلاعات مختلف برای شناسایی رویدادها را می‌توان از پایگاه‌داده، سیستم عامل، سرورهای وب یا فایل‌های رویدادنگاری استخراج کرد. جمع‌آوری مصنوعات و شواهد می‌تواند سبب تغییر در پایگاه‌داده شود. از این‌رو، پیش از استخراج اطلاعات از داخل یا خارج پایگاه‌داده می‌بایست نسبت به پایدار یا ناپایدار بودن اطلاعات آگاهی پیدا کرد. هر پایگاه‌داده شواهد مربوط به اعمال مختلف را در بخش‌ها و فایل‌های رویدادنگاری مختلف ذخیره می‌کند. این بدان معناست که به منظور تجزیه و تحلیل جرم‌شناسی می‌بایست نسبت به چگونگی عملکرد پایگاه‌داده، محل فایل‌ها و مصنوعات مختلف اطلاع داشت. از آنجا که تمرکز ما در فرآیند جرم‌شناسی پایگاه‌داده تنها بر روی اطلاعات حاصل از رویدادنگاری و ممیزی در پایگاه‌داده است، لذا اطلاعات مورد هدف برای گردآوری تنها به پایگاه‌داده محدود شده و شامل اطلاعات موجود در سیستم عامل و حافظه‌ی اصلی نمی‌باشد.

درصورتی که بر روی فایل‌های رویدادنگاری و ممیزی به صورت دوره‌ای اطلاعاتی ثبت شود، به هنگام شناسایی رویداد غیرمجاز می‌بایست ابتدا سرور پایگاه‌داده متوقف شود تا از اجرای پرسمان‌های جدید بر روی سرور خودداری گردد. بدین ترتیب از نگاشته شدن بر روی اطلاعات ثبت شده در فایل‌های رویدادنگاری و ممیزی جلوگیری می‌شود. در نهایت نیز به منظور انجام تحلیل‌های آتی می‌توان از فایل‌های مورد نیاز، یک نسخه‌ی پشتیبان تهیه نمود [۱۲].

مرحله جمع‌آوری اطلاعات و شواهد، شامل دو گام زیر می‌باشد:

۱. **تعیین نحوه‌ی جمع‌آوری اطلاعات:** در صورت مشاهده علائمی از وقوع رویداد غیرمجاز در پایگاه‌داده، با توجه به نوع رویداد می‌توان از منابع مختلفی برای جمع‌آوری اطلاعات استفاده کرد. به

---

[2] System Identifier [5]

عنوان نمونه، برای جمع‌آوری اطلاعات مربوط به برخی از رویدادها می‌بایست از رویدادهای ثبت‌شده در فایل‌های رویدادنگاری و برای برخی دیگر می‌بایست از تعریف خط‌مشی‌هایی ممیزی استفاده کرد.

۲. **بررسی تنظیمات فعلی:** پس از آنکه منابع جمع‌آوری اطلاعات برای یک رویداد ناخواسته مشخص شدند، تنظیمات فعلی سیستم بررسی می‌شود. با بررسی اولیه‌ی تنظیمات مشخص می‌شود که آیا اقدامات اولیه برای ثبت اطلاعات قبل از وقوع رویداد انجام شده‌اند یا خیر. به عنوان نمونه، بررسی می‌شود که آیا در پایگاه‌داده، خط‌مشی‌هایی برای ثبت اطلاعات ممیزی مربوط به جرم تعریف شده است یا خیر.

استخراج و تجزیه و تحلیل اطلاعات:

در این مرحله ابتدا ابزارها و پرسمان‌های هدف به منظور استخراج اطلاعات از منابع تعیین می‌شوند. یک روش محبوب در میان تحلیل‌گران جرم‌شناسی، استخراج عبارات SQL اجرا شده در پایگاه‌داده است. همچنین بی‌شک یکی از المان‌های بسیار مهم در تجزیه و تحلیل جرم‌شناسی، شناسایی هویت مجرم است. هر عملی که ثبت می‌شود را باید بتوان به یک شخص واقعی نسبت داد [۱۵]. سپس اطلاعات هدف از منابع مشخص شده استخراج و مرحله بررسی و تحلیل اطلاعات آغاز می‌گردد. در این مرحله با بررسی و تحلیل داده‌های جمع‌آوری شده، اطلاعاتی همچون عامل وقوع رویداد، زمان وقوع، دلایل وقوع، نوع تغییر حاصل از اجرای رویداد، داده متأثر از تغییر و چگونگی اعمال رویداد غیرمجاز، آشکار می‌شود [۱۰, ۱۱]. لازم به ذکر است که تجمیع داده‌ها در فرآیند جرم‌شناسی پایگاه‌داده بسیار حائز اهمیت است. به منظور سادگی در بررسی هر یک از رویدادهای ناخواسته، بخش استخراج اطلاعات و تجزیه و تحلیل با یکدیگر ادغام شده و تحت عنوان استخراج و تجزیه و تحلیل اطلاعات بیان می‌شود.

ترمیم:

پس از محرز شدن رخداد جرم در سامانه پایگاه‌داده، متناسب با نیاز و شواهد اطلاعاتی موجود، ممکن است ترمیم پایگاه‌داده امکان‌پذیر باشد. در واقع، ترمیم سامانه پایگاه‌داده بدین معناست که وضعیت پایگاه‌داده را به وضعیتی پیش از وقوع رویداد برگردانیم. به عنوان نمونه، در صورتی که داده‌های حساس از یک جدول حذف شده باشند، این مرحله به بازیابی داده‌های حذفی می‌پردازد.

ارائه‌ی مستندات:

در گام نهایی می‌بایست کلیه‌ی بررسی‌های صورت پذیرفته را در یک قالب استاندارد از پیش تعیین شده به نحوی مستند نمود که قابل ارائه به مدیریت سازمانی یا دادگاه قانونی برای طرح دعوی باشد. مستندسازی به سایر بررسی‌کنندگانی که سناریوی مشابه‌ای را تجربه می‌کنند نیز کمک خواهد کرد. به منظور ارائه مستندات مربوط به رویدادهای غیرمجاز کشف‌شده در سامانه، فرم استاندارد زیر ارایه شده است.

جدول ۱: تهیه‌ی مستند از فرآیند جرم‌شناسی پایگاه‌داده

عنوان رویداد			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی			
منابع رویدادنگاری			
شیوه یا ابزار تحلیل			
امکان ترمیم			

۲-۳ رهنمون‌های فرآیند جرم‌شناسی

در این بخش، برخی از مهم‌ترین رهنمون‌های مربوط به مراحل مختلف فرآیند جرم‌شناسی پایگاه‌داده آورده شده است. لازم به ذکر است که ملاحظات ذکر شده در این بخش برای هر سامانه پایگاه‌داده در هر سازمانی حیاتی است. با این وجود، ممکن است متناسب با نوع سازمان و نوع سامانه پایگاه‌داده، ملاحظات دیگری نیز افزوده شود [۱۲-۱۵].

۱. در صورت بروز نقض امنیتی، کل سازمان باید از آن مطلع شده و نشست آموزشی کوتاهی در زمینه رسیدگی به آن با حضور تمامی افراد برگزار شود. در صورتی که اطلاع‌رسانی به بخش‌های مختلف سازمان و تجزیه و تحلیل جرم‌شناسی توسط بخش‌های مختلف، طبق برنامه‌ی مشخصی انجام نشود، بخش‌هایی ممکن است موضوع را نادیده بگیرند و بخش‌های دیگری ممکن است آن را به اطلاع عموم برسانند. بنابراین، هرآنچه که در روند جرم‌شناسی انجام می‌شود می‌بایست طبق برنامه از پیش تدوین شده، صورت پذیرد.
۲. یکی از چالشی‌ترین مسائل در بررسی پایگاه‌های داده آن است که هر چه بیشتر در پایگاه‌داده جستجو و بررسی انجام شود، تغییرات بیشتری در آن رخ می‌دهد. لازم به ذکر است که تقریباً هر عملی که در پایگاه‌داده انجام می‌شود، می‌تواند باعث تغییر در رکوردهای دیکشنری شود.
۳. استفاده از حساب کاربری با مجوزهای بالا می‌تواند خود زمینه ایجاد تغییرات در پایگاه‌داده را فراهم آورد. بنابراین، در نظر گرفتن حساب کاربری با دسترسی‌های محدود فقط خواندنی برای این منظور

ایده‌آل است. اگر چنین حساب‌های کاربری قبل از وقوع جرم تعریف نشده باشد، ایجاد حساب کاربری جدید توصیه نمی‌شود؛ چرا که خود موجب تغییرات جدیدی در سامانه می‌شود و با وجود اینکه استفاده از کاربر SYS می‌تواند خطرناک باشد ولی منطقی‌تر است.

۴. برای قابل قبول بودن شواهد در دادگاه قانونی به هنگام طرح دعوی، دو اصل اساسی باید رعایت شود: ۱): اولین اصل آن است که می‌بایست ثابت شود که اطلاعات و شواهد گردآوری شده به صورت قانونی به دست آمده است و ۲): دومین اصل نیز آن است که می‌بایست ثابت شود که به هنگام جمع‌آوری شواهد و اطلاعات تغییری در آنها اعمال نشده است. برای اثبات اصل اول، پیش از جمع‌آوری شواهد باید قانونی بودن آن‌ها بررسی و تأیید شود. همچنین اصل دوم نیز با مستندسازی شواهد و اعمال اجرا شده بر روی آن‌ها قابل اثبات است. در حقیقت جمع‌آوری شواهد باید طی گام‌های از پیش تدوین شده‌ای صورت گیرد تا اطمینان حاصل شود که شواهد جمع‌آوری شده، تغییر نکرده‌اند. برای اثبات صحت داده‌ها می‌توان از روش مجموع مقابله‌ای[۶] استفاده کرد. این روش می‌تواند بر روی شواهد مختلف از جمله یک فایل یا کل دیسک سخت افزاری اعمال شود. با این روش می‌توان ثابت کرد که شواهد جمع‌آوری شده همان اطلاعاتی است که در ادامه از آن‌ها برای تجزیه و تحلیل استفاده می‌شود و بدون تغییر به دادگاه قابل ارائه است. توجه به این نکته حائز اهمیت است که برای استفاده از روش مجموع مقابله‌ای نباید به راحتی از بسته‌های موجود در پایگاه‌های داده استفاده شود. به عنوان مثال، در پایگاه‌داده اوراکل، نباید از بسته‌ی DBMS_SQLHASH استفاده شود چون ممکن است خود این بسته توسط مهاجم تغییر داده شده باشد. بنابراین در طول بررسی‌های جرم‌شناسی باید بتوان اعتبار ابزارها و عدم تغییر آن‌ها را ثابت کرد. مهاجم همچنین می‌تواند دیدهای موجود در پایگاه‌داده را برای مخفی نگه داشتن اعمال خود تغییر دهد. بنابراین باید یا از جدول‌های پایه در بررسی‌های جرم‌شناسی استفاده شود و یا پیش از استفاده از دیدها از صحت آن‌ها اطمینان حاصل گردد.

۵. یکی از مصنوعات مهم پایگاه‌داده برای تجزیه و تحلیل جرم‌شناسی، رویدادهای ثبت شده توسط ممیزی است. استفاده از ممیزی این اطمینان را ایجاد می‌کند که همیشه شواهدی برای استفاده در تحلیل جرم‌شناسی وجود دارد. می‌توان پایگاه‌داده را برای ثبت رویدادهای مشخص همچون ایجاد یک کاربر، تغییر رمز عبور و دسترسی به محتوای یک جدول تنظیم کرد. در صورتی که ممیزی فعال نباشد می‌توان از سایر قابلیت‌های رویدادنگاری در پایگاه‌های داده برای ثبت تغییرات استفاده کرد. با این وجود، به کارگیری ممیزی با جزئیات کافی و ثبت تمامی اعمال اجرا شده توسط مهاجم، تجزیه

---

[2] Checksum [6]

و تحلیل جرم‌شناسی را ساده‌تر می‌کند. تنظیمات مربوط به ممیزی می‌بایست بر اساس برنامه‌ای از قبل تعیین شده، مشخص گردد. در واقع بر اساس این برنامه، هرآنچه که نیاز به دانستن است، مشخص می‌گردد. در ادامه، برخی از امکان‌ها برای انجام تنظیمات ممیزی ارایه شده‌اند:

- افرادی که به پایگاه‌داده وارد یا از آن خارج می‌شوند.
- افرادی که خود را به جای مدیر پایگاه‌داده نمایش می‌دهند.
- تلاش برای حمله‌ی تزریق SQL[۲۷]
- تغییر در پروفایل کاربر
- تغییر در ساختار پایگاه‌داده

یک راه حل جامع برای تهیه‌ی ممیزی باید شامل ممیزی از خود ممیزی نیز باشد. در صورتی که مهاجم تلاش به حذف یک رکورد ممیزی کند، باید این عمل ثبت شود. همچنین تلاش برای تغییر تنظیمات ممیزی نیز باید ثبت گردد. در صورتی که ممیزی در پایگاه‌داده فعال باشد، اولین گام شناسایی تنظیمات ممیزی است. پس از آن می‌توان به رویدادهای ممیزی و استفاده از آن‌ها در بررسی‌های جرم‌شناسی پرداخت.

۶. شواهد و اطلاعات مربوط به جرم‌شناسی اغلب در مکان‌های مختلفی از پایگاه‌داده وجود دارند. شناخت شواهد و اطلاعات مهم و اولویت‌بندی آنها از اهمیت بالایی برخوردار است. به غیر از اطلاعاتی که می‌توان از طریق اجرای پرسمان بر روی پایگاه‌داده‌ی تغییریافته به‌دست‌آورد، می‌توان از طریق ابزارهایی که توسط سامانه پایگاه‌داده استفاده می‌شوند؛ همچون نهان‌گاه طرح اجرایی[۲۸] و رویدادنگاری تراکنش‌ها[۲۹] نیز شواهدی را جمع‌آوری کرد. یک طرح اجرایی، کارآمدترین روش اجرای درخواست‌های داده است که در نهان‌گاه طرح اجرایی برای استفاده‌ی مجدد ذخیره می‌شوند. رویدادنگاری تراکنش‌ها در شناخت پرسمان‌های اجرا شده بر روی پایگاه‌داده و برای بررسی‌ها و تحقیقات مختلف، مفید است. سایر منابع شامل فایل‌هایی هستند که تاریخچه‌ی مربوط به پایگاه‌داده را ذخیره می‌کنند. برخی از این فایل‌ها به طور اختصاصی در پایگاه‌داده کاربرد دارند، همچون فایل رویدادنگاری پایگاه‌داده و فایل‌های داده در حالی که سایر فایل‌ها همچون رویدادنگاری سرور وب و رویدادنگاری رویدادهای سیستمی یک سیستم‌عامل به طورخاص به سرور پایگاه‌داده اختصاص داده

---

2 SQL Injection
2 Execution plan cache
2 Transaction logs
7
8
9

نمی‌شوند. در هنگام تصمیم‌گیری درمورد اینکه کدام داده اول جمع‌آوری شود، مهم است که سطح بی‌ثباتی یک فایل در نظر گرفته شود.

۷. یکی از بزرگترین مسائل در تجزیه و تحلیل جرم‌شناسی در پایگاه‌داده آن است که به صورت معمول پایگاه‌های داده، رویدادهای مربوط به دسترسی و خواندن محتوای جداول را ثبت نمی‌کنند ولی در تمامی مواقع، تغییرات در پایگاه‌داده همچون بروزرسانی، درج و حذف داده‌ها ثبت می‌شوند. گاهی نیاز است که شواهدی برای بررسی سرقت داده‌ها شناسایی شود. سرقت داده‌ها، ممکن است به نحوی باشد که داده‌ها را از پایگاه‌داده حذف نکند. بنابراین می‌بایست به دنبال شواهدی برای دسترسی به داده‌ها از طریق پایگاه‌داده بود. دسترسی به این گونه شواهد معمولاً پیچیده است مگر اینکه ممیزی فعال باشد. در حقیقت تنها روشی که می‌توان از آن به طور حتم برای اثبات دسترسی به داده مشخص استفاده کرد، فعال کردن ممیزی روی آن پیش از دسترسی است. به طور طبیعی، ثبت فعالیت خواندن داده‌ها ایده‌آل است هرچند همیشه انجام نمی‌شود. بنابراین باید بتوان در کنار آن، از راه‌های جایگزین نیز استفاده کرد. بدین منظور اصولاً از همبستگی[۳۰]میان شواهد استفاده می‌شود. به عنوان مثال، در پایگاه‌داده اوراکل، ممکن است شواهدی مبنی بر ورود مهاجم و ایجاد اتصال به پایگاه‌داده وجود داشته باشد. مهاجم ممکن است پرسمان SELECT را وارد کرده باشد و بهینه‌ساز[۳۱]ر اوراکل وارد عملی برای کامپایل دستور SQL شده باشد. همچنین در صورتی که حمله بلافاصله مورد بررسی قرار گرفته باشد، پرسمان SQL استفاده شده توسط مهاجم ممکن است در SGA وجود داشته باشد. در این شرایط، در صورتی که حمله از طریق سرور وب انجام شده باشد، پرسمان SQL ممکن است در فایل رویدادنگاری مربوط به برنامه‌ی کاربردی تحت وب موجود باشد. بنابراین در صورتی که ممیزی بر روی سیستم فعال نباشد، باید از همبستگی میان شواهد مختلف برای نتیجه‌گیری درمورد سرقت اطلاعات استفاده شود.

۸. برای جلوگیری از حجیم شدن فایل‌های رویدادنگاری و ممیزی می‌توان خط‌مشی‌هایی را برای بازنویسی[۳۲]رویدادها در این گونه از فایل‌ها اعمال کرد. به عنوان مثال می‌توان مشخص کرد که در صورتی که حجم فایل‌های رویدادنگاری به ۱۰۰ مگابایت رسید، اطلاعات جدید از ابتدای فایل بر روی اطلاعات قبلی نوشته شود یا در یک دوره هفت روزه، فایل‌های رویدادنگاری جدید ایجاد شوند. درصورتی که بر روی فایل‌های رویدادنگاری و ممیزی به صورت دوره‌ای اطلاعات ثبت شود، هنگام تشخیص رویداد غیرمجاز، باید ابتدا سرور پایگاه‌داده متوقف شود تا از اجرای اعمال و پرسمان‌های

---

30 Correlation
31 Optimizer
32 Rotate

جدید بر روی سرور خودداری شود. سپس می‌توان از فایل‌های مورد نیاز، نسخه‌ی پشتیبان تهیه کرد تا تحلیل‌های آتی بر روی نسخه‌های پشتیبان انجام شود.

۹. در صورتی که خط‌مشی‌هایی برای تهیه‌ی پشتیبان از پایگاه‌داده به صورت دوره‌ای وجود داشته باشد، وضعیت مطلوبی که پایگاه‌داده پیش از این، در آن قرار داشته است در دسترس خواهد بود. در نتیجه، در صورت وقوع رویداد غیرمجاز با بازگرداندن فایل‌های پشتیبان می‌توان به حالت مطلوب پیش از رویداد غیرمجاز تغییر وضعیت داد.

۱۰. در صورت وجود فایل‌های رویدادنگاری و ممیزی بر روی سیستمی که در آن پایگاه‌داده وجود دارد، مدیر پایگاه‌داده یا کاربر مخرب می‌تواند به طور موقت تهیه‌ی ممیزی و رویدادنگاری را متوقف کرده و اعمال مورد نظر خود را اجرا کند و یا تغییراتی را به صورت دستی در فایل‌های ممیزی و رویدادنگاری ایجاد کند. در صورتی که چندین نسخه از داده‌های حساس در مکان‌های مختلف وجود داشته باشد، امکان از دست رفتن داده‌های حساس در صورت حذف آن‌ها از یک مکان، کاهش می‌یابد. همچنین مطلوب است که تمامی رویدادها به سیستم مرکزی ارسال شده و از آن‌ها به طور مرکزی حفاظت و نگهداری شود.

۱۱. معمولاً مهاجمین پس از حمله به پایگاه‌داده، سعی به حذف ردپای خود در فایل‌های رویدادنگاری و ممیزی می‌کنند. بنابراین محدود کردن دسترسی به این فایل‌ها و کپی‌برداری از آن‌ها و ذخیره‌سازی در سرور مرکزی از اهمیت زیادی برخوردار است. همچنین با تشخیص اعمال تغییر غیرمجاز در فایل‌های رویدادنگاری و ممیزی می‌توان متوجه شد که رویدادهای ثبت شده در این فایل‌ها فاقد اعتبار هستند. به عنوان نمونه، هنگام اجرای پرسمان بر روی فایل‌های رویدادنگاری redo log مربوط به پایگاه‌داده اوراکل، در صورتی که به صورت دستی تغییری در این فایل‌ها اعمال شده باشد، یکی از خطاهای موجود در شکل ۲ و شکل ۳ نشان داده می‌شود که نشان‌دهنده‌ی تغییر غیرمجاز در این فایل‌ها و عدم اعتبار اطلاعات ذخیره شده، است.

```
ORA-00308: cannot open archived log 'C:\Users\Desktop\oracle\oradata\orcl\REDO02.LOG'
ORA-27046: file size is not a multiple of logical block size
OSD-04012: file size mismatch (OS 209715713)
00308. 00000 -  "cannot open archived log '%s'"
*Cause:    The system cannot access a required archived redo log file.
*Action:   Check that the off line log exists, the storage device is
           online, and the archived file is in the correct location.
           Then attempt to continue recovery or restart the recovery
           session.
```

شکل ۲: خطای تغییر غیرمجاز در فایل رویدادنگاری

```
ORA-00368: checksum error in redo log block
ORA-00353: log corruption near block 132010 change 21987320 time 02/02/2018 10:11:30
ORA-00334: archived log: 'C:\USERS\DESKTOP\ORACLE\ORADATA\ORCL\REDO02.LOG'
00368. 00000 - "checksum error in redo log block"
*Cause:    The redo block indicated by the accompanying error, is not
           vaild. It has a checksum that does not match the block contents.
*Action:   Do recovery with a good version of the log or do time based
           recovery up to the indicated time. If this happens when archiving,
           archiving of the problem log can be skipped by clearing the log
           with the UNARCHIVED option. This must be followed by a backup of
           every datafile to insure recoverability of the database.
*Action:   Restore correct file or reset logs.
```

شکل ۳: خطای تغییر غیرمجاز در فایل رویدادنگاری

۲-۴ جمع‌بندی

در این فصل، ابتدا بستر مورد نیاز برای جرم‌شناسی پایگاه‌داده را تحت عنوان تمهیدات جرم‌شناسی به طور مشروح مورد بحث و بررسی قرار دادیم. سپس فرآیند جرم‌شناسی را از شناسایی جرم تا تهیه و ارائه مستندات به مدیریت سازمان و دادگاه‌قانونی برای طرح دعوی تشریح کردیم. همچنین به منظور ارائه مستندات مربوط به رویدادهای غیرمجاز کشف‌شده در سامانه، فرم استاندارد زیر ارایه گردید.

جدول ۲: تهیه‌ی مستند از فرآیند جرم‌شناسی پایگاه‌داده

عنوان رویداد			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی			
منابع رویدادنگاری			
شیوه یا ابزار تحلیل			
امکان ترمیم			

۳ درج، حذف و مشاهده‌ی غیرمجاز محتوای جداول

در این فصل به بحث و بررسی رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شوند و موجب درج سطر (های) جدید، حذف سطر (های)

موجود یا مشاهده تمامی یا بخشی از جدول (ها) در پایگاه‌داده می‌گردند، پرداخته می‌شود. سه رویداد فوق از جمله دستورات دستکاری داده (DML)[۳۳] در پایگاه‌داده به حساب می‌آیند. از آنجاییکه رویدادهای مورد بحث در این فصل از نقطه نظر جرم‌شناسی به هم نزدیک هستند، لذا تنها بر روی رویداد حذف غیرمجاز به عنوان یک نماینده از این رویدادها متمرکز شده و در صورت نیاز تفاوت‌های دیگر رویدادها ذکر می‌گردد.

۳-۱ شناسایی جرم

فرآیند جرم‌شناسی با مشاهده‌ی رویدادهای غیرمجاز در سامانه آغاز می‌شود. بنابراین در صورتیکه مدیر پایگاه‌داده خود به طور مستقیم یا غیر مستقیم (از طریق کاربران)، نسبت به حذف داده‌ها از جدولی آگاهی پیدا کند که انتظار حذف آنها در شرایط فعلی را نداشته است، فرآیند جرم‌شناسی در سامانه آغاز می‌شود.

۳-۲ جمع‌آوری اطلاعات و شواهد

از آنجاییکه هر پایگاه‌داده شواهد مربوط به اعمال مختلف را در بخش‌ها و فایل‌های رویدادنگاری مختلف ذخیره می‌کند، در این بخش قصد داریم منابع مربوط به شواهد و اطلاعات برای رویداد غیرمجاز حذف را تعیین نماییم. لازم به ذکر است که تمرکز ما در فرآیند جرم‌شناسی پایگاه‌داده تنها بر روی اطلاعات حاصل از رویدادنگاری و ممیزی در پایگاه‌داده است و شامل اطلاعات موجود در سیستم عامل و حافظه‌ی اصلی نمی‌باشد. از این‌رو، در ادامه به معرفی منابع مربوط به شواهد رویداد غیرمجاز حذف و نحوه آگاهی و تنظیم آنها می‌پردازیم.

رویدادنگاری تکمیلی: به صورت پیش‌فرض، اطلاعات مختصری در فایل‌های رویدادنگاری redo log ثبت می‌شوند. درصورتی‌که نیاز به ثبت داده‌های بیشتری باشد، باید از رویدادنگاری تکمیلی استفاده کرد. رویدادنگاری تکمیلی دارای دو سطح پایگاه‌داده و جدول به قرار زیر است [۳]:

- **پایگاه‌داده:** این سطح چندین نوع از رویدادنگاری تکمیلی از جمله حداقل رویدادنگاری تکمیلی[۳۴] را فراهم می‌کند. حداقل رویدادنگاری تکمیلی، سربار قابل توجهی بر روی پایگاه‌داده برای تولید فایل‌های redo log وارد نمی‌کند.
- **جدول:** رویدادنگاری تکمیلی در سطح جدول مشخص می‌کند که از کدامیک از ستون‌های جدول به‌طور موثر رکوردهای ثبت تهیه شود.

---

[3] Data Manipulation Language [3]
[3] Minimal supplemental logging [4]

در صورتی که حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده فعال باشد، با استفاده از رویدادهای ثبت‌شده در فایل‌های log redo و از طریق ابزار LogMiner می‌توان به اطلاعات مفیدی از جمله داده‌های حذف‌شده، کاربر اجراکننده‌ی پرسمان و زمان حذف اطلاعات دسترسی پیدا کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات رویدادنگاری تکمیلی و نحوه فعال کردن آن آورده شده است.

جدول ۳: بررسی وضعیت و فعال کردن رویدادنگاری تکمیلی برای رویداد حذف در سطح پایگاه‌داده

بررسی فعال بودن حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده
SELECT SUPPLEMENTAL_LOG_DATA_MIN FROM V$DATABASE;
فعال کردن حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

ممیزی یکپارچه: در صورتی که ممیزی یکپارچه فعال باشد و همچنین خط‌مشی‌ای برای تهیه‌ی ممیزی از رویداد حذف، تعریف و فعال شده باشد، می‌توان شواهدی را برای رویداد حذف از این طریق بدست آورد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات ممیزی یکپارچه، نحوه فعال کردن آن و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۴: بررسی وضعیت و فعال کردن رویدادنگاری ممیزی یکپارچه برای رویداد حذف

بررسی فعال بودن ممیزی یکپارچه		
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';		
فعال کردن ممیزی یکپارچه		
net stop <OracleServiceName>	متوقف کردن پایگاه‌داده	۱
lsnrctl status | find "Alias"	یافتن نام شنونده	۲
lsnrctl stop <ListenerName>	متوقف کردن شنونده	۳
ORACLE_HOME%/bin/orauniaud12.dll.dbl To: ORACLE_HOME%/bin/orauniaud12.dll	تغییر نام فایل	۴
lsnrctl start <ListenerName>	راه‌اندازی مجدد شنونده	۵
net start <OracleServiceName>	راه‌اندازی مجدد پایگاه‌داده	۶
تعریف خط‌مشی برای تهیه‌ی ممیزی از عمل حذف		

۱	ایجاد خط‌مشی ممیزی یکپارچه	CREATE AUDIT POLICY table_delete_data ACTIONS DELETE;
۲	فعال کردن خط‌مشی	AUDIT POLICY table_delete_data BY SYS, test;
	برخی دستورات سودمند	
۱	فهرست خط‌مشی‌های فعال	SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES;
۲	مشاهده تعریف خط‌مشی‌های فعال	SELECT * FROM AUDIT_UNIFIED_POLICIES WHERE POLICY_NAME LIKE 'TABLE_%';

ممیزی ریزدانه: در صورت تعریف خط‌مشی در ممیزی ریزدانه برای عملیات حذف بر روی جدول با داده‌های حساس، در شرایطی که نیاز به بررسی داده‌های حذفی از جدول باشد، می‌توان با اجرای پرسمان بر روی دید UNIFIED_AUDIT_TRAIL به خروجی‌های مورد نظر دسترسی پیدا کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات ممیزی ریزدانه، نحوه تعریف خط‌مشی و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۵: بررسی وضعیت و فعال کردن رویدادنگاری ممیزی ریزدانه برای رویداد حذف

	بررسی فعال بودن ممیزی ریزدانه	
		SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Fine-grained Auditing';
	تعریف خط‌مشی برای تهیه‌ی ممیزی از عمل حذف	

		BEGIN
		DBMS_FGA.ADD_POLICY(
		object_schema => 'test',
		object_name => 'info',
		policy_name => 'table_info_delete',
		enable => TRUE,
		statement_types => 'INSERT, UPDATE, SELECT, DELETE') ;
		END;

	برخی دستورات سودمند	
۱	مشاهده خط‌مشی‌های فعال	SELECT * FROM ALL_AUDIT_POLICIES WHERE ENABLED='YES';

۳-۳ استخراج و تجزیه و تحلیل اطلاعات

در این قسمت نحوه‌ی استخراج اطلاعات برای هر یک از منابع مربوط به شواهد و اطلاعات مورد بحث و بررسی قرار می‌گیرد. با استفاده از اطلاعات جمع‌آوری شده، تحلیل‌گر باید داده‌های حذف‌شده را بررسی و در صورت مشاهده‌ی رویداد حذف غیرمجاز، آن را به عنوان جرم/عیب شناسایی نماید. در ادامه برای هر یک از منابع حاوی شواهد و اطلاعات برای رویدادهای سامانه، نحوه استخراج و تجزیه و تحلیل شواهد تشریح می‌گردد.

رویدادنگاری تکمیلی: با استفاده از اطلاعات استخراج‌شده از فایل‌های رویدادنگاری تکمیلی می‌توان اطلاعاتی در مورد زمان حذف داده، کاربر اجراکننده‌ی پرسمان حذف و پرسمان‌هایی برای اجرای مجدد[۳۵] و بازگشت به عقب[۳۶] دست آورد. برای استخراج اطلاعات از فایل‌های رویدادنگاری redo log می‌توان از ابزار LogMiner استفاده کرد. برای این منظور گام‌های ذکر شده در جدول زیر را به ترتیب دنبال کنید.

جدول ۶: استخراج و تحلیل اطلاعات رویدادنگاری تکمیلی برای رویداد حذف

استخراج و تحلیل اطلاعات رویدادنگاری تکمیلی		
۱	تعیین فایل‌های redo log برای تحلیل	EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => ORACLE_HOME\oracle\oradata\orcl\REDO01.LOG', OPTIONS => DBMS_LOGMNR.NEW); EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => 'ORACLE_HOME \oracle\oradata\orcl\REDO02.LOG', OPTIONS => DBMS_LOGMNR.ADDFILE); EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => 'ORACLE_HOME\oracle\oradata\orcl\REDO03.LOG', OPTIONS => DBMS_LOGMNR.ADDFILE);
۲	راه‌اندازی LogMiner	EXECUTE DBMS_LOGMNR.START_LOGMNR(OPTIONS => DBMS_LOGMNR.DICT_FROM_ONLINE_CATALOG);
۳	مشاهده شواهد از داده‌های حذف شده یک جدول	SELECT TIMESTAMP, USERNAME, SQL_REDO, SQL_UNDO, TABLE_NAME, OPERATION FROM v$logmnr_contents WHERE TABLE_NAME = ‘TABLE_NAME’ and OPERATION='DELETE';

[3] Redo
[3] Undo
[5]
[6]

برخی دستورات مفید		
۱	تنظیم دقیق زمان وقوع رویداد با دقت ثانیه	ALTER SESSION SET NLS_DATE_FORMAT = 'DD-MON-YYYY HH24:MI:SS';

ممیـــزی یکپارچـــه: بـا اسـتفاده از اطلاعـات استخراج‌شـده از ممیـزی یکپارچـه، پرسـمان اجرایـی، کـاربر اجراکننده‌ی پرسمان و زمان اجرای پرسمان مشخص می‌شود. در جدول زیر، دستورات مربوط به اسـتخراج و تحلیل اطلاعات و شواهد وقوع جرم با استفاده از پیکره‌بندی ممیزی یکپارچه آورده شده است.

جدول ۷: استخراج و تحلیل اطلاعات رویدادنگاری ممیزی یکپارچه برای رویداد حذف

استخراج و تحلیل اطلاعات ممیزی یکپارچه		
۱	مشاهده شواهد داده‌های حذف شده ثبت شده توسط یک خط‌مشی	SELECT UNIFIED_AUDIT_POLICIES, DBUSERNAME, SQL_TEXT, EVENT_TIMESTAMP, CURRENT_USER FROM UNIFIED_AUDIT_TRAIL WHERE SQL_TEXT LIKE 'delete%' and UNIFIED_AUDIT_POLICIES='TABLE_DELETE_DATA';
برخی دستورات مفید		
۱	اطمینان از انتقال تمامی رکوردهای ممیزی بر روی دیسک	EXEC SYS.DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL;

ممیزی ریزدانه: با استفاده از اطلاعات استخراج‌شده از ممیزی ریزدانه، پرسمان اجرایی، کـاربر اجراکننـده‌ی پرسمان و زمان اجرای پرسمان مشخص می‌شود. در جـدول زیـر، دسـتورات مربـوط بـه اسـتخراج و تحلیـل اطلاعات و شواهد وقوع جرم با استفاده از پیکره‌بندی ممیزی ریزدانه آورده شده است.

جدول ۸: استخراج و تحلیل اطلاعات رویدادنگاری ممیزی ریزدانه برای رویداد حذف

استخراج و تحلیل اطلاعات ممیزی ریزدانه		
۱	مشاهده شواهد داده‌های حذف شده	SELECT FGA_POLICY_NAME, DBUSERNAME, SQL_TEXT, EVENT_TIMESTAMP, CURRENT_USER FROM UNIFIED_AUDIT_TRAIL

WHERE SQL_TEXT LIKE 'delete%' and FGA_POLICY_NAME != 'null';		

۳-۴ ترمیم

در صورتی که پیش از حذف داده‌ها اقدامات لازم جهت تهیه فایل پشتیبان صورت پذیرفته باشد، با بازیابی فایل می‌توان اطلاعات از دست رفته را مجدداً در اختیار گرفت. در این بخش سعی داریم روش‌هایی به غیر از روش‌های مربوط به تهیه‌ی نسخه‌های پشتیبان را برای بازیابی داده‌های از دست رفته مورد بحث و بررسی قرار دهیم.

ترمیم با LogMiner : همانطور که در بخش‌های قبلی بیان گردید می‌توان اطلاعات و شواهدی را در مورد داده‌های حذف‌شده از طریق فایل‌های redo log و ابزار LogMiner به دست آورد. در خروجی ابزار LogMiner، ستونی به نام SQL_UNDO وجود دارد که پرسمان لازم برای بازیابی داده‌ی حذف‌شده را نشان می‌دهد. یک راه برای بازگرداندن داده‌های حذف‌شده، یافتن تمامی‌داده‌های حذف‌شده از یک جدول و بازیابی آن‌ها از طریق پرسمان موجود در ستون SQL_UNDO است.

ترمیم با قابلیت FLASHBACK : قابلیت FLASHBACK یک ویژگی بسیار مطلوب در پایگاه‌داده اوراکل است که این امکان را فراهم می‌آورد تا وضعیت اشیا یا کل پایگاه‌داده به وضعیت مطلوبی در زمان گذشته بازگردد. در صورت فعال بودن این ویژگی بر روی پایگاه‌داده، با استفاده از پرسمان FLASHBACK می‌توان داده‌های فعلی را با داده‌های گذشته مقایسه کرد. لازم به ذکر است که در صورت اجرای دستور FLASHBACK توسط کاربر SYS، خطایی مشابه شکل ۴ از سوی سامانه پایگاه‌داده تولید می‌شود که نشان‌دهنده‌ی آن است که دستور FLASHBACK برای کاربر SYS پشتیبانی نمی‌شود. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن FLASHBACK ، نحوه فعال کردن آن، بازیابی اطلاعات و برخی از دستورات سودمند در این رابطه آورده شده است.

```
Error starting at line : 35 in command -
FLASHBACK TABLE test TO TIMESTAMP TO_TIMESTAMP('22-JAN-2018 21:46:48', 'DD-MON-YYYY HH24:MI:SS')
Error report -
SQL Error: ORA-08185: Flashback not supported for user SYS
08185. 00000 -  "Flashback not supported for user SYS"
*Cause:    user logged on as SYS
*Action:   logon as a different (non SYS) user.
```

شکل ۴: عدم امکان استفاده از قابلیت Flashback توسط کاربر SYS

جدول ۹: بررسی وضعیت و ترمیم با قابلیت FLASHBACK برای رویداد حذف

ترمیم با قابلیت FLASHBACK

۱	بررسی وضعیت قابلیت FLASHBACK	SELECT flashback_on FROM v$database;
۲	اطلاع از وضعیت یک جدول در زمان مشخص	SELECT * FROM test AS OF TIMESTAMP TO_TIMESTAMP('22-JAN-2018 21:46:48', 'DD-MON-YYYY HH24:MI:SS');
۳	بازیابی داده‌های از دست رفته	ALTER TABLE [TBALE_NAME] ENABLE ROW MOVEMENT; FLASHBACK TABLE [TBALE_NAME] TO TIMESTAMP TO_TIMESTAMP('22-JAN-2018 21:46:48', 'DD-MON-YYYY HH24:MI:SS');
فعال کردن قابلیت FLASHBACK پایگاه‌داده		
۱	قراردهی پایگاه‌داده در حالت ARCHIVELOG پیش از فعال‌سازی قابلیت FLASHBACK پایگاه‌داده	ARCHIVE LOG LIST SHUTDOWN IMMEDIATE; STARTUP MOUNT; ALTER DATABASE ARCHIVELOG; ALTER DATABASE OPEN;
۲	پیکربندی ناحیه‌ی بازیابی سریع[۳۷]	ALTER SYSTEM SET db_recovery_file_dest_size = '80000M'; ALTER SYSTEM SET db_recovery_file_dest='ORACLE_HOME\oracle\arch';
۳	پیکربندی پارامتر DB_flashback_retention_target	ALTER SYSTEM SET DB_FLASHBACK_RETENTION_TARGET=1440 ;
۴	فعال‌سازی FLASHBACK	ALTER DATABASE FLASHBACK ON;
برخی دستورات مفید		
۱	دستور جایگزین برای بازیابی داده‌های از دست رفته	INSERT INTO [TABLE_NAME] (SELECT * FROM [TABLE_NAME] AS OF TIMESTAMP TO_TIMESTAMP('22-JAN-2018 21:46:48', 'DD-MON-YYYY HH24:MI:SS'));

[3] Fast recovery area [7]

۳-۵ ارائه‌ی مستندات

در این گام، اطلاعات کسب شده در طول فرآیند جرم‌شناسی پایگاه‌داده مستند می‌شود. برای این منظور می‌بایست برای هر یک از رویدادهای درج، حذف و مشاهده جداول در پایگاه‌داده به هنگام بررسی جرم، جداول زیر را به طور دقیق تکمیل و به مدیریت سازمان برای پیگیری‌های لازم و طرح دعوی ارائه کرد.

جدول ۱۰: تهیه‌ی مستند از فرآیند جرم‌شناسی رویداد درج غیرمجاز در جدول

درج غیرمجاز در جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐	استفاده از قابلیت Flashback ☐	
توضیحات			

جدول ۱۱: تهیه‌ی مستند از فرآیند جرم‌شناسی رویداد حذف غیرمجاز محتوای جدول

حذف غیرمجاز محتوای جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐	استفاده از قابلیت Flashback ☐	
توضیحات			

جدول ۱۲: تهیه‌ی مستند از فرآیند جرم‌شناسی رویداد مشاهده غیرمجاز محتوای جدول

مشاهده غیرمجاز محتوای جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐

شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐	
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐	
امکان ترمیم	استفاده از LogMiner ☐	استفاده از قابلیت Flashback ☐
توضیحات		

۳-۶ جمع‌بندی

در این فصل به بحث و بررسی رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شوند و موجب درج سطر (های) جدید، حذف سطر (های) موجود یا مشاهده تمامی یا بخشی از جدول (ها) در پایگاه می‌گردند، پرداختیم. برای این منظور، پس از شناسایی جرم، سه رویکرد برای جمع‌آوری شواهد و اطلاعات مربوط به جرم به نام‌های رویدادنگاری تکمیلی، ممیزی یکپارچه و ممیزی ریزدانه را معرفی کردیم. برای هر یک از این رویکردها، تنظیمات مربوط به فعال‌سازی، استخراج اطلاعات و شواهد، تحلیل شواهد، ترمیم و در پایان تهیه مستندات را تشریح کردیم.

۴ بروزرسانی غیرمجاز محتوای جداول

در این فصل به بحث و بررسی رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال و موجب تغییر داده‌های پایگاه‌داده می‌شوند، می‌پردازیم.

۴-۱ شناسایی جرم

فرآیند جرم‌شناسی با مشاهده‌ی رویدادهای غیرمجاز در سامانه آغاز می‌شود. بنابراین در صورتی که مدیر پایگاه‌داده خود به طور مستقیم یا غیرمستقیم (از طریق کاربران)، نسبت به تغییر و دستکاری برخی از داده‌های جدولی آگاهی پیدا کند که انتظار تغییر آنها در شرایط فعلی را نداشته است، فرآیند جرم‌شناسی در سامانه آغاز می‌شود.

۴-۲ جمع‌آوری اطلاعات و شواهد

از آنجایی که هر پایگاه‌داده شواهد مربوط به اعمال مختلف را در بخش‌ها و فایل‌های رویدادنگاری مختلف ذخیره می‌کند، در این بخش قصد داریم منابع مربوط به شواهد رویداد بروزرسانی غیرمجاز را تعیین نماییم. لازم به ذکر است که تمرکز ما در فرآیند جرم‌شناسی پایگاه‌داده تنها بر روی اطلاعات حاصل از رویدادنگاری و

ممیزی در پایگاه‌داده است و شامل اطلاعات موجود در سیستم عامل و حافظه‌ی اصلی نمی‌باشد. از این‌رو، در ادامه به معرفی منابع مربوط به شواهد رویداد بروزرسانی غیرمجاز و نحوه آگاهی و تنظیم آنها می‌پردازیم.

رویدادنگاری تکمیلی: در صورتی که حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده فعال باشد، با استفاده از رویدادهای ثبت‌شده در فایل‌های redo log و از طریق ابزار LogMiner می‌توان به اطلاعات مفیدی از جمله داده‌های بروزرسانی شده، کاربر اجراکننده‌ی پرسمان و زمان بروزرسانی داده‌ها دسترسی پیدا کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات رویدادنگاری تکمیلی در سطح پایگاه‌داده و نحوه فعال کردن آن آورده شده است.

جدول ۱۳: بررسی وضعیت و فعال کردن رویدادنگاری تکمیلی برای بروزرسانی غیرمجاز محتوای جداول در سطح پایگاه‌داده

بررسی فعال بودن حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده
SELECT SUPPLEMENTAL_LOG_DATA_MIN FROM V$DATABASE;
فعال کردن حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

همچنین در صورتی که رویدادنگاری تکمیلی در سطح جدول فعال شده باشد، اطلاعات دقیق‌تری از سطر تغییر یافته نظیر مقادیر سایر ستون‌ها را می‌توان به دست آورد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات رویدادنگاری تکمیلی در سطح جدول و نحوه فعال کردن آن آورده شده است.

جدول ۱۴: بررسی وضعیت و فعال کردن رویدادنگاری تکمیلی برای بروزرسانی غیرمجاز محتوای جداول در سطح جدول

بررسی فعال بودن حداقل رویدادنگاری تکمیلی در سطح جدول
SELECT * FROM DBA_LOG_GROUPS WHERE TABLE_NAME='<TABLE_NAME>';
فعال کردن حداقل رویدادنگاری تکمیلی در سطح جدول
ALTER TABLE <TABLE_NAME> ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;

ممیزی یکپارچه: در صورتی که ممیزی یکپارچه فعال باشد و همچنین خط‌مشی‌ای برای تهیه‌ی ممیزی از رویداد بروزرسانی تعریف و فعال شده باشد، می‌توان شواهدی را برای رویداد بروزرسانی از این طریق بدست آورد. ممیزی در حقیقت اطلاعاتی در مورد کاربر اجراکننده‌ی پرسمان و زمان اجرای پرسمان ارائه می‌دهد

ولی با استفاده از اطلاعات ثبت شده توسط ممیزی نمی‌توان سطرهایی که توسط پرسمان UPDATE دستکاری شده‌اند را پیدا کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات ممیزی یکپارچه، نحوه فعال کردن آن و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۱۵: بررسی وضعیت و فعال کردن ممیزی یکپارچه برای بروزرسانی غیرمجاز محتوای جداول

بررسی فعال بودن ممیزی یکپارچه		
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';		
فعال کردن ممیزی یکپارچه		
net stop <OracleServiceName>	متوقف کردن پایگاه‌داده	۱
lsnrctl status | find "Alias"	یافتن نام شنونده	۲
lsnrctl stop <ListenerName>	متوقف کردن شنونده	۳
ORACLE_HOME%/bin/orauniaud12.dll.dbl To: ORACLE_HOME%/bin/orauniaud12.dll	تغییر نام فایل	۴
lsnrctl start <ListenerName>	راه‌اندازی مجدد شنونده	۵
net start <OracleServiceName>	راه‌اندازی مجدد پایگاه‌داده	۶
تعریف خط‌مشی برای تهیه‌ی ممیزی از عمل به‌روزرسانی		
CREATE AUDIT POLICY table_update_data ACTIONS UPDATE;	ایجاد خط‌مشی ممیزی یکپارچه	۱
AUDIT POLICY table_update_data BY SYS, test;	فعال کردن خط‌مشی	۲
برخی دستورات سودمند		
SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES;	فهرست خط‌مشی‌های فعال	۱
SELECT * FROM AUDIT_UNIFIED_POLICIES WHERE POLICY_NAME LIKE 'TABLE_%';	مشاهده تعریف خط‌مشی‌های فعال	۲

ممیزی ریزدانه: در صورت تعریف خط‌مشی در ممیزی ریزدانه برای عملیات بروزرسانی بر روی جداول با داده‌های حساس، در شرایطی که نیاز به بررسی داده‌های بروزرسانی شده از جدول باشد، می‌توان با اجرای پرسمان بر روی دید UNIFIED_AUDIT_TRAIL به خروجی‌های مورد نظر دسترسی پیدا کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات ممیزی ریزدانه، نحوه فعال کردن آن و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۱۶: بررسی وضعیت و فعال کردن ممیزی ریزدانه برای بروزرسانی غیرمجاز محتوای جداول

بررسی فعال بودن ممیزی ریزدانه		
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Fine-grained Auditing';		
تعریف خط‌مشی برای تهیه‌ی ممیزی از عمل به‌روزرسانی		

BEGIN
DBMS_FGA.ADD_POLICY(
object_schema => 'test',
object_name => 'info',
policy_name => 'table_info_update',
enable => TRUE,
statement_types => 'INSERT, UPDATE, SELECT, DELETE') ;
END;		

برخی دستورات سودمند		
SELECT * FROM ALL_AUDIT_POLICIES WHERE ENABLED='YES';	مشاهده خط‌مشی‌های فعال	۱

۳-۴ استخراج و تجزیه و تحلیل اطلاعات

در این قسمت نحوه‌ی استخراج اطلاعات برای هر یک از منابع مربوط به شواهد اطلاعات مورد بحث و بررسی قرار می‌گیرد. با استفاده از اطلاعات جمع‌آوری‌شده، تحلیل‌گر باید داده‌های بروزرسانی شده را بررسی و در صورت مشاهده‌ی رویداد غیرمجاز، آن را به عنوان جرم/عیب شناسایی نماید. در ادامه برای هر یک از منابع، نحوه استخراج و تجزیه و تحلیل شواهد بررسی می‌گردد.

رویدادنگاری تکمیلی: با استفاده از اطلاعات استخراج‌شده از فایل‌های رویدادنگاری تکمیلی می‌توان اطلاعاتی در مورد زمان بروزرسانی داده، کاربر اجراکننده‌ی پرسمان و پرسمان‌هایی برای اجرای مجدد[۳۸] و بازگشت به عقب[۳۹] دست آورد. برای استخراج اطلاعات از فایل‌های رویدادنگاری redo log می‌توان از ابزار LogMiner استفاده کرد. برای این منظور لازم است گام‌های ذکر شده در جدول زیر به ترتیب دنبال شود.

[3] Redo
[3] Undo
[8]
[9]

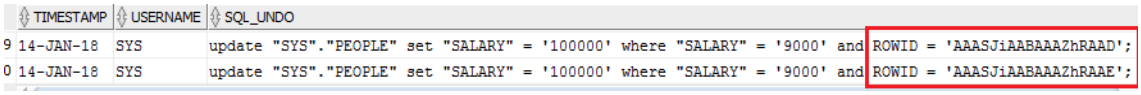
جدول ۱۷: استخراج و تحلیل اطلاعات رویدادنگاری تکمیلی برای بروزرسانی غیرمجاز محتوای جداول

استخراج و تحلیل اطلاعات رویدادنگاری تکمیلی		
EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => ORACLE_HOME\oracle\oradata\orcl\REDO01.LOG', OPTIONS => DBMS_LOGMNR.NEW); EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => 'ORACLE_HOME \oracle\oradata\orcl\REDO02.LOG', OPTIONS => DBMS_LOGMNR.ADDFILE); EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => 'ORACLE_HOME\oracle\oradata\orcl\REDO03.LOG', OPTIONS => DBMS_LOGMNR.ADDFILE);	تعیین فایل‌های redo log برای تحلیل	۱
EXECUTE DBMS_LOGMNR.START_LOGMNR(OPTIONS => DBMS_LOGMNR.DICT_FROM_ONLINE_CATALOG);	راه‌اندازی LogMiner	۲
SELECT TIMESTAMP, USERNAME, SQL_REDO, SQL_UNDO, TABLE_NAME, OPERATION FROM v$logmnr_contents WHERE TABLE_NAME = '<TABLE_NAME>' and OPERATION='UPDATE';	مشاهده شواهد از داده‌های به‌روزرسانی شده یک جدول	۳
برخی دستورات مفید		
ALTER SESSION SET NLS_DATE_FORMAT = 'DD-MON-YYYY HH24:MI:SS';	تنظیم دقیق زمان وقوع رویداد با دقت ثانیه	۱

با استفاده از دستور زیر می‌توان داده‌های بروزرسانی شده در یک جدول مشخص را استخراج کرد.

```
SELECT TIMESTAMP, USERNAME, SQL_UNDO, TABLE_NAME, OPERATION FROM v$logmnr_contents WHERE TABLE_NAME=' <TABLE_NAME> ' and
OPERATION='UPDATE';
```

همانگونه که در شکل ۵ دیده می‌شود با استفاده از اطلاعات موجود در فایل‌های رویدادنگاری و مقدار ROWID می‌توان سطرهای تغییر داده‌شده را شناسایی کرد.



	TIMESTAMP	USERNAME	SQL_UNDO
9	14-JAN-18	SYS	update "SYS"."PEOPLE" set "SALARY" = '100000' where "SALARY" = '9000' and ROWID = 'AAASJiAABAAAZhRAAD';
0	14-JAN-18	SYS	update "SYS"."PEOPLE" set "SALARY" = '100000' where "SALARY" = '9000' and ROWID = 'AAASJiAABAAAZhRAAE';

شکل ۵: استخراج اطلاعات (داده‌های به‌روزرسانی شده) موجود در فایل‌های redo log

با استفاده از مقدار شناسه‌ی هر سطر می‌توان سطرهای بروزرسانی شده را تشخیص داد، به عنوان مثال برای نمونه ارایه شده در بالا، سطرهایی با شناسه‌ی یکتای یک و دو، مقدار ستون salary آن‌ها از ۱۰۰۰۰۰ به ۹۰۰۰ تغییر داده‌شده است.

```
SELECT ROWID,<list_of_column_names> FROM people;
```

	ROWID	ID	SALARY	NAME
1	AAASJiAABAAAZhRAAD	1	9000	s n
2	AAASJiAABAAAZhRAAE	2	9000	z h
3	AAASJiAABAAAZhRAAF	3	400000	a n

شکل ۶: نمایش محتوای یک جدول

همچنین در صورتی که رویدادنگاری تکمیلی در سطح جدول فعال شده باشد، اطلاعات دقیق‌تری از سطر تغییر یافته شامل مقادیر سایر ستون‌ها را می‌توان با دستور زیر بدست آورد. در شکل ۷، مقادیر تمامی ستون‌ها در سطر بروزرسانی شده، مشخص شده‌اند.

```
SELECT TIMESTAMP, USERNAME, SQL_UNDO, TABLE_NAME, OPERATION FROM
    v$logmnr_contents WHERE TABLE_NAME=' TABLE_NAME ' and OPERATION='UPDATE';
```

```
14-JAN-18  SYS   update "SYS"."PEOPLE" set "SALARY" = '9000' where "ID" = '1' and "SALARY" = '100000' and "NAME" = 's n' and ROWID = 'AAASJiAABAAAZhRAAD
14-JAN-18  SYS   update "SYS"."PEOPLE" set "SALARY" = '9000' where "ID" = '2' and "SALARY" = '100000' and "NAME" = 'z h' and ROWID = 'AAASJiAABAAAZhRAAE
```

شکل ۷: رویدادنگاری تکمیلی و اطلاعات دقیق‌تر درمورد سطرهای به‌روزرسانی شده

ممیزی یکپارچه: با استفاده از اطلاعات استخراج‌شده از ممیزی یکپارچه، اطلاعاتی نظیر پرسمان اجرایی، کاربر اجراکننده‌ی پرسمان و زمان اجرای پرسمان مشخص می‌شود ولی نمی‌توان با استفاده از اطلاعات ممیزی به سطرهایی که با پرسمان UPDATE، بروزرسانی شده‌اند، دست یافت. در جدول زیر، دستورات مربوط به استخراج و تحلیل اطلاعات و شواهد وقوع جرم با استفاده از پیکربندی ممیزی یکپارچه آورده شده است.

جدول ۱۸: استخراج و تحلیل اطلاعات ممیزی یکپارچه برای بروزرسانی غیرمجاز محتوای جداول

استخراج و تحلیل اطلاعات ممیزی یکپارچه		
۱	مشاهده شواهد داده‌های بروزرسانی شده توسط یک	SELECT UNIFIED_AUDIT_POLICIES, DBUSERNAME, SQL_TEXT, EVENT_TIMESTAMP FROM UNIFIED_AUDIT_TRAIL WHERE SQL_TEXT LIKE 'update%' and

	خط‌مشی	UNIFIED_AUDIT_POLICIES='TABLE_UPDATE_DATA';
برخی دستورات مفید		
۱	اطمینان از انتقال تمامی رکوردهای ممیزی بر روی دیسک	EXEC SYS.DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL;

ممیزی ریزدانه: با استفاده از اطلاعات استخراج شده از ممیزی ریزدانه، اطلاعاتی نظیر پرسمان اجرایی، کاربر اجراکننده‌ی پرسمان و زمان اجرای پرسمان مشخص می‌شود ولی نمی‌توان با استفاده از اطلاعات ممیزی به سطرهایی که با پرسمان UPDATE، بروزرسانی شده‌اند، دست یافت. در جدول زیر، دستورات مربوط به استخراج و تحلیل اطلاعات و شواهد وقوع جرم با استفاده از پیکربندی ممیزی ریزدانه آورده شده است.

جدول ۱۹: استخراج و تحلیل اطلاعات ممیزی ریزدانه برای بروزرسانی غیرمجاز محتوای جداول

استخراج و تحلیل اطلاعات ممیزی ریزدانه		
۱	مشاهده شواهد داده‌های بروزرسانی شده	SELECT FGA_POLICY_NAME, DBUSERNAME, SQL_TEXT, EVENT_TIMESTAMP FROM UNIFIED_AUDIT_TRAIL WHERE SQL_TEXT LIKE 'update%' and FGA_POLICY_NAME != 'null';

۴-۴ ترمیم

در صورتی که از رویدادهای ثبت‌شده در فایل‌های redo log برای استخراج اطلاعات استفاده شود، با توجه به شناسه‌ی یکتای سطر تغییر داده‌شده و پرسمان موجود در ستون SQL_UNDO می‌توان داده‌های بروزرسانی شده را به حالت قبل بازگرداند.

۴-۵ ارائه‌ی مستندات

در این گام، اطلاعات کسب شده در طول فرآیند جرم‌شناسی پایگاه‌داده مستند می‌شود. برای این منظور می‌بایست برای رویداد بروزرسانی داده‌های جداول به هنگام بررسی جرم، جدول زیر به طور دقیق تکمیل و به مدیریت سازمان برای پیگیری‌های لازم و طرح دعوی ارائه گردد.

جدول ۲۰: تهیه‌ی مستند از فرآیند جرم‌شناسی رویداد بروزرسانی غیرمجاز محتوای جدول

بروزرسانی غیرمجاز محتوای جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐		
توضیحات			

۴-۶ جمع‌بندی

در این فصل به بحث و بررسی رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال می‌شوند و موجب بروزرسانی داده‌های جداول در پایگاه‌داده می‌گردند، پرداخته شد. برای این منظور، پس از شناسایی جرم، سه رویکرد برای جمع‌آوری شواهد و اطلاعات مربوط به جرم به نام‌های رویدادنگاری تکمیلی، ممیزی یکپارچه و ممیزی ریزدانه معرفی گردید. در پایان نیز برای هر یک از این رویکردها، تنظیمات مربوط به فعال‌سازی، استخراج اطلاعات و شواهد، تحلیل شواهد، ترمیم و در پایان تهیه مستندات تشریح شد.

۵ تغییر غیرمجاز شمای پایگاه‌داده

در این فصل به بحث و بررسی رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال و موجب تغییر در شمای پایگاه‌داده می‌شود، می‌پردازیم. این دسته از رویدادها، از جمله دستورات تعریف داده (DDL)[۴] در پایگاه‌داده به حساب می‌آیند. از آنجاییکه رویدادهای مورد بحث در این فصل از نقطه نظر جرم‌شناسی بسیار به هم نزدیک هستند، لذا تنها بر روی رویداد حذف غیرمجاز یک جدول متمرکز می‌شویم.

[4] Data Definition Language

۵-۱ شناسایی جرم

فرآیند جرم‌شناسی با مشاهده‌ی رویدادهای غیرمجاز در سامانه آغاز می‌شود. بنابراین در صورتیکه مدیر پایگاه‌داده خود به طور مستقیم یا غیرمستقیم (از طریق کاربران)، نسبت به تغییر در شمای پایگاه‌داده همچون حذف یک جدول آگاهی پیدا کند که انتظار تغییر آن در شرایط فعلی را نداشته است، فرآیند جرم‌شناسی در سامانه آغاز می‌شود.

۵-۲ جمع‌آوری اطلاعات و شواهد

از آنجاییکه هر پایگاه‌داده شواهد مربوط به اعمال مختلف را در بخش‌ها و فایل‌های رویدادنگاری مختلف ذخیره می‌کند، در این بخش قصد داریم منابع مربوط به شواهد رویداد حذف غیرمجاز یک جدول را تعیین نماییم. لازم به ذکر است که تمرکز ما در فرآیند جرم‌شناسی پایگاه‌داده تنها بر روی اطلاعات حاصل از رویدادنگاری و ممیزی در پایگاه‌داده است و شامل اطلاعات موجود در سیستم عامل و حافظه‌ی اصلی نمی‌باشد. از این‌رو در ادامه به معرفی منابع مربوط به شواهد رویداد حذف غیرمجاز یک جدول و نحوه آگاهی و تنظیم آن‌ها می‌پردازیم.

رویدادنگاری DDL : فایل رویدادنگاری مربوط به اعمال DDL، شامل عبارات DDL اجراشده توسط کاربران پایگاه‌داده است. این فایل دارای فرمت XML است. درصورتی‌که پارامتر ENABLE_DDL_LOGGING مقدار TRUE داشته باشد، عبارات DDL در فایل مربوط به رویدادنگاری DDL ثبت می‌شوند. مقدار این پارامتر به صورت پیش‌فرض FALSE است [۱۸]. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن رویدادنگاری DDL، نحوه فعال کردن آن و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۲۱: بررسی وضعیت و فعال کردن رویدادنگاری DDL برای تغییر غیرمجاز شمای پایگاه‌داده

بررسی فعال بودن رویدادنگاری DDL		
SELECT * FROM V$PARAMETER WHERE name = 'enable_ddl_logging';		
فعال کردن رویدادنگاری DDL		
ALTER SYSTEM SET enable_ddl_logging=true;		
برخی دستورات سودمند		
SELECT VALUE FROM V$DIAG_INFO WHERE NAME = 'ADR Home';	یافتن مسیر فایل رویدادنگاری DDL (این فایل در زیر دایرکتوری log/ddl قرار دارد)	۱

رویدادنگاری تکمیلی: در صورتی که حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده فعال باشد، با استفاده از رویدادهای ثبت‌شده در فایل‌های redo log و از طریق ابزار LogMiner می‌توان به اطلاعات مفیدی از جمله جدول حذف شده، کاربر اجراکننده‌ی پرسمان و زمان حذف جدول دسترسی پیدا کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات رویدادنگاری تکمیلی و نحوه فعال کردن آن آورده شده است.

جدول ۲۲: بررسی وضعیت و فعال کردن رویدادنگاری تکمیلی برای تغییر غیرمجاز شمای پایگاه‌داده

بررسی فعال بودن حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده
SELECT SUPPLEMENTAL_LOG_DATA_MIN FROM V$DATABASE;
فعال کردن حداقل رویدادنگاری تکمیلی در سطح پایگاه‌داده
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

ممیزی یکپارچه: در صورتی که ممیزی یکپارچه فعال باشد و همچنین خط‌مشی‌ای برای تهیه‌ی ممیزی از رویداد حذف جدول تعریف و فعال شده باشد، می‌توان شواهدی را برای رویداد حذف جدول از این طریق بدست آورد. خط‌مشی ممیزی یکپارچه با توجه به نوع عمل DDL تعریف می‌شود. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن تنظیمات ممیزی یکپارچه، نحوه فعال کردن آن و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۲۳: بررسی وضعیت و فعال کردن ممیزی یکپارچه برای تغییر غیرمجاز شمای پایگاه‌داده

بررسی فعال بودن ممیزی یکپارچه		
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';		
فعال کردن ممیزی یکپارچه		
net stop <OracleServiceName>	متوقف کردن پایگاه‌داده	۱
lsnrctl status | find "Alias"	یافتن نام شنونده	
lsnrctl stop <ListenerName>	متوقف کردن شنونده	۲
ORACLE_HOME%/bin/orauniaud12.dll.dbl To: ORACLE_HOME%/bin/orauniaud12.dll	تغییر نام فایل	۳
lsnrctl start <ListenerName>	راه‌اندازی مجدد شنونده	۴
net start <OracleServiceName>	راه‌اندازی مجدد پایگاه‌داده	۵

تعریف خط‌مشی برای تهیه‌ی ممیزی از عمل حذف جدول		
۱	ایجاد خط‌مشی ممیزی یکپارچه	CREATE AUDIT POLICY ddl_info ACTIONS ALTER TABLE, CREATE TABLE, DROP TABLE;
۲	فعال کردن خط‌مشی	AUDIT POLICY ddl_info;
برخی دستورات سودمند		
۱	فهرست خط‌مشی‌های فعال	SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES;
۲	مشاهده خط‌مشی‌های فعال	SELECT * FROM AUDIT_UNIFIED_POLICIES WHERE POLICY_NAME LIKE 'TABLE_%';

۵-۳ استخراج و تجزیه و تحلیل اطلاعات

در این قسمت نحوه‌ی استخراج اطلاعات از منابع مربوط به شواهد، مورد بحث و بررسی قرار می‌گیرد. با استفاده از اطلاعات جمع‌آوری شده، تحلیل‌گر باید تغییرات در شمای پایگاه‌داده را بررسی و در صورت مشاهده‌ی رویداد غیرمجاز، آن را به عنوان جرم/عیب شناسایی نماید. در ادامه برای هر یک از منابع حاوی شواهد و اطلاعات مربوط به رویدادهای سامانه، نحوه استخراج و تجزیه و تحلیل اطلاعات تشریح می‌گردد.

رویدادنگاری DDL : با استفاده از اطلاعات استخراج‌شده از فایل‌های رویدادنگاری DDL می‌توان اطلاعاتی در مورد زمان حذف جدول و پرسمان اجرا شده به دست آورد. همانطور که در شکل زیر دیده می‌شود، کاربر اجراکننده‌ی پرسمان در این فایل ثبت نمی‌شود.

```
<msg time='2018-09-02T22:10:23.955+04:30' org_id='oracle' comp_id='rdbms'
 msg_id='opiexe:4695:2946163730' type='UNKNOWN' group='diag_adl'
 level='16' host_id='TESTUSER-PC' host_addr='fe80::e45f:c4ed:7de2:2364%26'
 pid='5780' con_uid='1' con_id='1'
 con_name='CDB$ROOT'>
 <txt>create table profile (name varchar(10), lastname varchar(20))
 </txt>
</msg>
<msg time='2018-09-02T22:20:58.659+04:30' org_id='oracle' comp_id='rdbms'
 msg_id='opiexe:4695:2946163730' type='UNKNOWN' group='diag_adl'
 level='16' host_id='TESTUSER-PC' host_addr='fe80::e45f:c4ed:7de2:2364%26'
 pid='5780' con_uid='1' con_id='1'
 con_name='CDB$ROOT'>
 <txt>drop table profile
 </txt>
```

شکل ۸: اطلاعات ثبت شده در فایل رویدادنگاری DDL

رویدادنگاری تکمیلی: با استفاده از اطلاعات استخراج‌شده از فایل‌های رویدادنگاری تکمیلی می‌توان اطلاعاتی در مورد زمان حذف جدول، کاربر اجراکننده‌ی پرسمان و پرسمان‌هایی برای اجرای مجدد[1] بدست آورد. برای استخراج اطلاعات از فایل‌های رویدادنگاری redo log[4] می‌توان از ابزار LogMiner استفاده کرد. برای این منظور می‌بایست گام‌های زیر را به ترتیب دنبال کرد.

جدول ۲۴: استخراج و تحلیل اطلاعات رویدادنگاری تکمیلی برای تغییر غیرمجاز شمای پایگاه‌داده

استخراج و تحلیل اطلاعات رویدادنگاری تکمیلی		
۱	تعیین فایل‌های redo log برای تحلیل	EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => ORACLE_HOME\oracle\oradata\orcl\REDO01.LOG', OPTIONS => DBMS_LOGMNR.NEW); EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => 'ORACLE_HOME \oracle\oradata\orcl\REDO02.LOG', OPTIONS => DBMS_LOGMNR.ADDFILE); EXECUTE DBMS_LOGMNR.ADD_LOGFILE(LOGFILENAME => 'ORACLE_HOME\oracle\oradata\orcl\REDO03.LOG', OPTIONS => DBMS_LOGMNR.ADDFILE);
۲	راه‌اندازی LogMiner	EXECUTE DBMS_LOGMNR.START_LOGMNR(OPTIONS => DBMS_LOGMNR.DICT_FROM_ONLINE_CATALOG);
۳	مشاهده شواهد از جدول حذف شده	SELECT TIMESTAMP, USERNAME, SQL_UNDO, TABLE_NAME, OPERATION, SQL_REDO FROM v$logmnr_contents WHERE OPERATION='DDL';
برخی دستورات مفید		
۱	تنظیم دقیق زمان وقوع رویداد با دقت ثانیه	ALTER SESSION SET NLS_DATE_FORMAT = 'DD-MON-YYYY HH24:MI:SS';

ممیزی یکپارچه: با استفاده از اطلاعات استخراج شده از ممیزی یکپارچه، اطلاعاتی نظیر پرسمان اجرایی، کاربر اجراکننده‌ی پرسمان و زمان اجرای پرسمان مشخص می‌شود. در جدول زیر، دستورات مربوط به استخراج و تحلیل اطلاعات و شواهد وقوع جرم با استفاده از پیکربندی ممیزی یکپارچه آورده شده است.

[4] Redo [1]

جدول ۲۵: استخراج و تحلیل اطلاعات ممیزی یکپارچه برای تغییر غیرمجاز شمای پایگاه‌داده

استخراج و تحلیل اطلاعات ممیزی یکپارچه		
۱	مشاهده شواهد جدول حذف شده	SELECT DBUSERNAME, SQL_TEXT, EVENT_TIMESTAMP, ACTION_NAME FROM UNIFIED_AUDIT_TRAIL WHERE UNIFIED_AUDIT_POLICIES='DDL_INFO' ORDER BY EVENT_TIMESTAMP;
برخی دستورات مفید		
۱	اطمینان از انتقال تمامی رکوردهای ممیزی بر روی دیسک	EXEC SYS.DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL;

۵-۴ ترمیم

در صورتی که پیش از تغییر در شمای پایگاه‌داده و به طور خاص حذف یک جدول، اقدامات لازم جهت تهیه فایل پشتیبان صورت پذیرفته باشد، با بازیابی فایل می‌توان اطلاعات از دست رفته را مجدداً در اختیار گرفت. در این بخش سعی داریم روش‌هایی به غیر از روش‌های مربوط به تهیه‌ی نسخه‌های پشتیبان را برای بازیابی جداول و داده‌های از دست رفته مورد بحث و بررسی قرار دهیم.

ترمیم پس از اجرای پرسمان غیرمجاز DROP TABLE: قابلیت RECYCLE BIN این امکان را در پایگاه‌داده‌ی Oracle فراهم کرده است که با حذف یک جدول، بلافاصله جدول به طور کامل پاک نشود بلکه در RECYCLE BIN قرار گیرد و قابل بازیابی باشد. البته RECYCLE BIN به صورت دوره‌ای و بنابر معیارهای مختلفی پاک می‌شود، همچنین می‌توان اطلاعات درون آن را دستی حذف کرد. قابلیت RECYCLE BIN به صورت پیش‌فرض فعال است. هر یک از کاربران، RECYCLE BIN مخصوص به خود را دارند. نکته‌ی بسیار مهم در مورد قابلیت RECYCLE BIN در Oracle این است که جدولی که در فضای جدول[۴] SYSTEM[۲] ایجاد شده است، پس از حذف در RECYCLE BIN قرار نمی‌گیرد و نمی‌توان آن را

4 Tablespace 2

بازیابی کرد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن قابلیت RECYCLE BIN، نحوه فعال کردن آن، بازیابی اطلاعات و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۲۶: بررسی وضعیت و فعال کردن ترمیم با قابلیت RECYCLE BIN برای رویداد تغییر غیرمجاز شمای پایگاه‌داده

ترمیم با قابلیت RECYCLE BIN		
۱	بررسی وضعیت قابلیت RECYCLE BIN	SELECT * FROM V$PARAMETER WHERE name='recyclebin'; SHOW PARAMETER recyclebin;
۲	فعال کردن قابلیت RECYCLE BIN	ALTER SYSTEM SET recyclebin = ON DEFERRED;
۳	مشاهده‌ی محتوای RECYCLE BIN مربوط به کاربر SYS	SELECT * FROM dba_recyclebin;
۴	مشاهده‌ی محتوای RECYCLE BIN مربوط به کاربر وارد شده به پایگاه‌داده	SELECT * FROM recyclebin;
۵	بازیابی جدول حذف شده	FLASHBACK TABLE <TABLE_NAME> TO BEFORE DROP;

ترمیم پس از اجرای پرسمان غیرمجاز TRUNCATE TABLE : با استفاده از قابلیت آرشیو داده‌های FLASHBACK[۴۳] می‌توان تغییرات در یک جدول را در طول زمان حیاتش ذخیره و ردگیری کرد. به صورت پیش‌فرض آرشیو داده‌های FLASHBACK برای هیچ جدولی فعال نیست. با فعال شدن قابلیت آرشیو داده‌های FLASHBACK بر روی یک جدول، تغییرات اعمال‌شده بر روی جدول در آرشیو FLASHBACK نوشته می‌شوند. در صورتی که دستور TRUNCATE بر روی جدول اجرا شود، می‌توان داده‌های موجود در جدول را بازیابی کرد.

---

4 Flashback Data Archives 3

در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن قابلیت آرشیو داده‌های FLASHBACK، نحـوه فعال کردن آن، بازیابی اطلاعات و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۲۷: فعال کردن قابلیت آرشیو داده‌های FLASHBACK بر روی یک جدول برای رویداد تغییر غیرمجاز شمای پایگاه‌داده

فعال کردن قابلیت آرشیو داده‌های FLASHBACK بر روی یک جدول		
۱	ایجاد یک فضای جدول مجزا برای ذخیره‌ی آرشیو داده‌های FLASHBACK	CREATE TABLESPACE tbs_arch DATAFILE 'ORACLE_HOME\oracle\flashback_archive.dbf' SIZE 10m;
۲	ایجاد آرشیو FLASHBACK در فضای جدول تعریف‌شده (برای مدت یک روز)	CREATE FLASHBACK ARCHIVE flashback_archive TABLESPACE tbs_arch RETENTION 1 DAY;
۳	نسبت دادن جدول یا جداول مورد نظر به آرشیو FLASHBACK تعریف شده	ALTER TABLE <TABLE_NAME> FLASHBACK ARCHIVE flashback_archive
ترمیم با قابلیت آرشیو داده‌های FLASHBACK		
۱	بررسی فعال بودن قابلیت آرشیو داده‌های FLASHBACK بر روی یک جدول	SELECT * FROM dba_flashback_archive_tables WHERE STATUS='ENABLED' and TABLE_NAME='<TABLE_NAME>';
۲	بازگرداندن جدول به زمانی در گذشته	INSERT INTO <TABLE_NAME> SELECT * FROM <TABLE_NAME> AS OF TIMESTAMP to_timestamp('28012018 20:50:34','ddmmyyyy hh24:mi:ss');
برخی دستورات مفید		
۱	فهرست آرشیوهای FLASHBACK تعریف شده	SELECT * FROM dba_flashback_archive_ts;

بازگرداندن پایگاه‌داده به نقطه‌ای از زمان: در صورتی که به طور تصادفی یا با قصد خرابکارانه تغییرات ناخواسته‌ای در پایگاه‌داده رخ دهد، با استفاده از قابلیت FLASHBACK پایگاه‌داده می‌توان کل پایگاه‌داده را به وضعیت مناسبی در گذشته بازگرداند. توجه به این نکته حائز اهمیت است که با فعال‌سازی این قابلیت،

تمامی تغییرات اعمال‌شده بر روی داده‌ها ثبت می‌شوند، چنانکه هر چه اعمال درج، بروزرسانی و حذف بیشتری انجام شود، سربار بیشتری به سامانه تحمیل خواهد شد. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن قابلیت FLASHBACK پایگاه‌داده، نحوه فعال کردن آن، بازیابی اطلاعات و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۲۸: فعال کردن قابلیت FLASHBACK پایگاه‌داده برای رویداد تغییر غیرمجاز شمای پایگاه‌داده

فعال کردن قابلیت FLASHBACK پایگاه‌داده		
۱	قراردهی پایگاه‌داده در حالت ARCHIVELOG پیش از فعال‌سازی قابلیت FLASHBACK پایگاه‌داده	ARCHIVE LOG LIST SHUTDOWN IMMEDIATE; STARTUP MOUNT; ALTER DATABASE ARCHIVELOG; ALTER DATABASE OPEN;
۲	پیکربندی ناحیه‌ی بازیابی سریع[۴۴]	ALTER SYSTEM SET db_recovery_file_dest_size = '80000M'; ALTER SYSTEM SET db_recovery_file_dest='ORACLE_HOME\oracle\arch';
۳	پیکربندی پارامتر DB_flashback_retention_target	ALTER SYSTEM SET DB_FLASHBACK_RETENTION_TARGET=1440 ;
۴	فعال‌سازی FLASHBACK پایگاه‌داده	ALTER DATABASE FLASHBACK ON;
ترمیم با قابلیت FLASHBACK پایگاه‌داده		
۱	خاموش کردن و توقف پایگاه‌داده	Shutdown immediate
۲	راه‌اندازی پایگاه‌داده در حالت mount	Startup mount
۳	بازیابی به SCN مشخص	FLASHBACK DATABASE TO SCN 12345;
۴	بازیابی به زمان مشخص	FLASHBACK DATABASE TO TIME "to_date('01/01/2016', 'dd/mm/yyyy')";
۵	بازیابی به نقطه بازیابی تعریف شده	FLASHBACK DATABASE TO RESTORE POINT test_restore_point;

[4] Fast recovery area [4]

۶	باز کردن مجدد پایگاه‌داده	ALTER DATABASE OPEN RESETLOGS;
برخی دستورات مفید		
۱	تعریف نقطه‌ی بازیابی برای پایگاه‌داده	CREATE RESTORE POINT test_restore_point GUARANTEE FLASHBACK DATABASE;
۲	فهرست نقاط بازیابی تعریف شده	SELECT NAME, SCN, TIME, DATABASE_INCARNATION#, GUARANTEE_FLASHBACK_DATABASE,STORAGE_SIZE FROM V$RESTORE_POINT
۳	بررسی وضعیت قابلیت FLASHBACK بر روی پایگاه‌های داده	SELECT NAME, FLASHBACK_ON FROM v$database;

۵-۵ ارائه‌ی مستندات

در این گام، اطلاعات کسب شده در طول فرآیند جرم‌شناسی پایگاه‌داده مستند می‌شود. برای این منظور می‌بایست به هنگام بررسی جرم، جدول زیر به طور دقیق تکمیل و به مدیریت سازمان برای پیگیری‌های لازم و طرح دعوی ارائه گردد.

جدول ۲۹: تهیه‌ی مستند از فرآیند جرم‌شناسی رویداد تغییر غیرمجاز شمای پایگاه‌داده

تغییر غیرمجاز شمای پایگاه‌داده				
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐	
شیوه ممیزی	ممیزی یکپارچه ☐			
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐	رویدادنگاری DDL ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐			
امکان ترمیم	استفاده از قابلیت Flashback ☐	آرشیو داده‌های Flashback ☐	استفاده از قابلیت RecycleBin ☐	
توضیحات				

۵-۶ جمع‌بندی

در این فصل به بحث و بررسی رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی بر روی پایگاه‌داده اعمال و موجب تغییر در شمای پایگاه‌داده می‌گردند، پرداخته شد. برای این منظور، پس از شناسایی جرم، سه رویکرد برای جمع‌آوری شواهد و اطلاعات مربوط به جرم به

نام‌های رویدادنگاری DDL، رویدادنگاری تکمیلی و ممیزی یکپارچه معرفی گردید. برای هر یک از این رویکردها، تنظیمات مربوط به فعال‌سازی، استخراج اطلاعات و شواهد، تحلیل شواهد، ترمیم و در پایان تهیه مستندات تشریح شد.

۶ تلاش برای ورود غیرمجاز به پایگاه‌داده

در این فصل، رویدادهای غیرمجازی که به صورت خصمانه یا ناخواسته توسط کاربر/برنامه‌کاربردی برای ورود به پایگاه‌داده صورت می‌پذیرد را مورد بحث و بررسی قرار می‌دهیم. در یک دسته‌بندی کلی، رویداد ورود غیرمجاز در دو دسته: ۱): تلاش برای ورود به پایگاه‌داده از طریق بدست آوردن نام کاربری و کلمه عبور و ۲): تلاش برای ورود به سمپاد از طریق بدست‌آوردن شناسه یکتای سیستم تقسیم‌بندی می‌شود. در ادامه این دو رویداد مورد بحث و بررسی قرار می‌گیرند.

۶-۱ شناسایی جرم

تلاش برای یافتن نام کاربری یا کلمه‌ی عبور: در صورتی که تلاش‌های ناموفق برای ورود به سیستم پایگاه‌داده ثبت شوند، با مشاهده‌ی رویدادهای ثبت‌شده می‌توان حمله به پایگاه‌داده برای یافتن نام کاربری یا کلمه‌ی عبور یک نام کاربری را تشخیص داد. در این شرایط فرآیند جرم‌شناسی در سامانه آغاز می‌شود.

تلاش برای یافتن شناسه‌ی یکتای سیستم: در صورتی که تلاش‌های ناموفق برای حدس SID ثبت شوند، با مشاهده‌ی رویدادهای ثبت‌شده در سامانه، می‌توان حمله به پایگاه‌داده برای یافتن SID را تشخیص داد. در این شرایط فرآیند جرم‌شناسی در سامانه آغاز می‌شود.

۶-۲ جمع‌آوری اطلاعات و شواهد

تلاش برای یافتن نام کاربری یا کلمه‌ی عبور: از آنجاییکه هر پایگاه‌داده شواهد مربوط به اعمال مختلف را در بخش‌ها و فایل‌های رویدادنگاری مختلف ذخیره می‌کند، در این بخش قصد داریم منابع مربوط به شواهد رویداد تلاش برای ورود به پایگاه‌داده را تعیین نماییم. لازم به ذکر است که تمرکز ما در فرآیند جرم‌شناسی پایگاه‌داده تنها بر روی اطلاعات حاصل از رویدادنگاری و ممیزی در پایگاه‌داده است و شامل اطلاعات موجود در سیستم عامل و حافظه‌ی اصلی نمی‌باشد.

به صورت پیش‌فرض خط‌مشی ora_logon_failures در سامانه، تلاش‌های ناموفق برای ورود به پایگاه‌داده را ثبت می‌کند. در جدول زیر، دستورات مربوط به بررسی فعال/غیرفعال بودن خط‌مشی ora_logon_failures، نحوه فعال کردن آن و برخی از دستورات سودمند در این رابطه آورده شده است.

جدول ۳۰: بررسی وضعیت و فعال کردن خط مشی ora_logon_failures برای ورود غیرمجاز از طرق تلاش برای یافتن نام‌کاربری و کلمه عبور

بررسی فعال بودن خط‌مشی ora_logon_failures		
SELECT * from AUDIT_UNIFIED_ENABLED_POLICIES;		
فعال کردن خط‌مشی پیش‌فرض ora_logon_failures		
AUDIT POLICY ora_logon_failures;		
برخی دستورات سودمند		
SELECT * FROM SYS.AUDIT_UNIFIED_POLICIES	لیست خط‌مشی‌های پیش‌فرض و تعریف شده	۱

تلاش برای یافتن شناسه‌ی یکتای سیستم: با استفاده از فایل رویدادنگاری مربوط به شنونده‌ی[۴۵] پایگاه‌داده می‌توان حمله‌ی حدس SID را تشخیص داد. با اجرای دستور lsnrctl status در خط فرمان[۴۶] می‌توان محل فایل رویدادنگاری مربوط به شنونده‌ی پایگاه‌داده را به دست آورد.

```
lsnrctl status | find "Listener Log File"
```

۳-۶ استخراج و تجزیه و تحلیل اطلاعات

تلاش برای یافتن نام کاربری یا کلمه‌ی عبور: در این قسمت نحوه‌ی استخراج اطلاعات مورد بحث و بررسی قرار می‌گیرد. با استفاده از اطلاعات جمع‌آوری شده، تحلیل‌گر باید تلاش‌های ناموفق برای ورود به پایگاه‌داده را بررسی و در صورت مشاهده‌ی تلاش‌های متوالی در فواصل زمانی کوتاه آن را به عنوان یک جرم/عیب تلقی نماید. هنگامی‌که نام کاربری یا کلمه‌ی عبور اشتباه وارد شود، کد خطای ۱۰۱۷ تولید خواهد شد.

جدول ۳۱: استخراج و تحلیل اطلاعات خط‌مشی ora_logon_failures **برای ورود غیرمجاز از طرق تلاش برای یافتن نام‌کاربری و کلمه عبور**

استخراج و تحلیل اطلاعات خط‌مشی ora_logon_failures

[4] Listener
[4] Command prompt
[5]
[6]

```
SELECT DBUSERNAME, EVENT_TIMESTAMP, ACTION_NAME, RETURN_CODE,
CURRENT_USER FROM unified_audit_trail
WHERE unified_audit_policies = 'ORA_LOGON_FAILURES'  AND return_code = 1017 ORDER
BY EVENT_TIMESTAMP;
```

تلاش برای یافتن شناسه‌ی یکتای سیستم: در فایل رویدادنگاری شنونده، می‌توان تلاش برای اتصال به شناسه‌ی یکتای سیستم را مشاهده کرد. هنگامی‌که در بازه‌های زمانی کوتاه، SID-های مختلف برای اتصال مورد آزمون قرار می‌گیرند، به نوعی تلاش برای یافتن SID پایگاه‌داده قوت می‌گیرد.

۶-۴ ترمیم

تلاش برای یافتن نام کاربری یا کلمه‌ی عبور: در صورتی که رویدادهای ثبت‌شده نشان‌دهنده‌ی تلاش برای ورود به پایگاه‌داده باشند، بر اساس صلاحدید مدیر پایگاه‌داده می‌توان حساب کاربری را برای مدتی قفل کرد. بدین ترتیب به نوعی حمله‌ی حدس کلمه‌ی عبور، دشوار و غیرممکن می‌شود و به هنگام ورود با نام کابری مورد نظر به کاربر خطا نشان داده می‌شود.

جدول ۳۲: قفل کردن نام کاربری برای ورود غیرمجاز از طرق تلاش برای یافتن نام‌کاربری و کلمه عبور

قفل کردن نام کاربری به صورت دستی		
ALTER USER <USERNAME> ACCOUNT LOCK;		
قفل کردن خودکار نام کاربری پس از تعدادی تلاش ناموفق برای ورود		
CREATE PROFILE test_profile LIMIT PASSWORD_LIFE_TIME 365 PASSWORD_GRACE_TIME 10 PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX 1 FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME UNLIMITED;	ایجاد پروفایل	۱
CREATE USER <USERNAME> IDENTIFIED BY flintstone PROFILE test_profile;	ایجاد کاربر با پروفایل تعریف شده	۲
برخی دستورات سودمند		

۱	خارج کردن نام کاربری از حالت قفل	ALTER USER <USERNAME> ACCOUNT UNLOCK;

تلاش برای یافتن شناسه‌ی یکتای سیستم: به منظور دشوارسازی فرآیند حدس SID بهتر است از کلمات و واژه‌های متداول که عموماً به عنوان SID استفاده می‌شوند، همچون orcle استفاده نشود.

۵-۶ ارائه‌ی مستندات

تلاش برای یافتن نام کاربری یا کلمه‌ی عبور: در این گام، اطلاعات کسب شده در طول فرآیند جرم‌شناسی پایگاه‌داده مستند می‌شود. برای این منظور می‌بایست به هنگام بررسی جرم، جدول زیر به طور دقیق تکمیل و به مدیریت سازمان برای پیگیری‌های لازم و طرح دعوی ارائه گردد.

جدول ۳۳: تهیه‌ی مستند از فرآیند جرم‌شناسی برای رویداد تلاش برای یافتن نام کاربری یا کلمه‌ی عبور

تلاش برای یافتن نام کاربری یا کلمه‌ی عبور			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	خط‌مشی ora_logon_failures ☐		
منابع رویدادنگاری	فاقد منبع رویدادنگاری است.		
شیوه یا ابزار تحلیل	استخراج محتوای unified_audit_trail همراه با کد بازگشتی ۱۰۱۷ ☐		
امکان ترمیم	قفل کردن نام کاربری دستی یا به صورت خودکار ☐		
توضیحات			

تلاش برای یافتن شناسه‌ی یکتای سیستم: در این گام، اطلاعات کسب شده در طول فرآیند جرم‌شناسی پایگاه‌داده مستند می‌شود. برای این منظور می‌بایست به هنگام بررسی جرم، جدول زیر به طور دقیق تکمیل و به مدیریت سازمان برای پیگیری‌های لازم و طرح دعوی ارائه گردد.

جدول ۳۴: تهیه‌ی مستند از فرآیند جرم‌شناسی برای رویداد تلاش برای یافتن شناسه‌ی یکتای سیستم

تلاش برای یافتن شناسه‌ی یکتای سیستم			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	فاقد شیوه ممیزی است.		

منابع رویدادنگاری	فایل رویدادنگاری مربوط به شنونده‌ی پایگاه‌داده ☐
شیوه یا ابزار تحلیل	فاقد شیوه یا ابزار تحلیل است.
امکان ترمیم	عدم استفاده از کلمات و واژه‌های متداول به عنوان SID ☐
توضیحات	

۶-۶ جمع‌بندی

در این فصل، تلاش برای ورود به پایگاه‌داده در صورت نداشتن نام کاربری یا کلمه‌ی عبور و همچنین تلاش برای ورود به پایگاه‌داده با حدس شناسه‌ی یکتای سیستم مورد بحث و بررسی قرار گرفت. برای این منظور، پس از شناسایی جرم، رویکردی برای جمع‌آوری شواهد و اطلاعات مربوط به جرم معرفی گردید. در پایان نیز برای رویکرد معرفی شده، تنظیمات مربوط به فعال‌سازی، استخراج اطلاعات و شواهد، تحلیل شواهد، ترمیم و تهیه مستندات تشریح شد.

۷ خلاصه مطالب

جرم‌شناسی پایگاه‌داده فرآیندی است که طی آن تلاش می‌شود تا اطلاعاتی چون زمان/ چگونگی/ چرایی و فرد مجرم برای یک رخداد غیرمجاز در سامانه مشخص شود. جرم‌شناسی پایگاه‌داده زمانی رخ می‌دهد که از مأمور ممیزی، کشف چگونگی وقوع نقض امنیتی و شخص مجرم درخواست شود. جرم‌شناسی پایگاه‌داده، چالش‌ها و مسائل زیادی به همراه دارد که آن را تبدیل به یک موضوع پیچیده کرده است.

با استفاده از مدل‌های فرآیند جرم‌شناسی پایگاه‌داده می‌توان به صورت ساختاریافته‌ای عملیات مربوط به جرم‌شناسی پایگاه‌داده را پیش برد. در مراحل مختلف فرآیند جرم‌شناسی، تمرکز اصلی بر روی پایگاه‌داده و اطلاعات موجود در آن برای شناسایی جرم است. در حقیقت تنها از اطلاعات ثبت‌شده در پایگاه‌های داده به منظور شناسایی جرم استفاده می‌شود و استفاده از اطلاعات ثبت‌شده بر روی سیستم عامل، داده‌های موجود در حافظه و شبکه، خارج از حوزه‌ی مورد بحث است. در یک دسته‌بندی کلی، جرم‌شناسی پایگاه‌داده شامل گام‌های زیر است:

۱. شناسایی جرم،
۲. جمع‌آوری اطلاعات و شواهد،
۳. استخراج اطلاعات و تجزیه و تحلیل،
۴. ترمیم،
۵. و ارائه‌ی مستندات.

هر سامانه پایگاه‌داده، شواهد مربوط به رویدادهای مختلف را در فایل‌های مختلف برای استفاده در تجزیه و تحلیل جرم‌شناسی ذخیره می‌کند. این به معنای آن است که برای تجزیه و تحلیل جرم‌شناسی باید نسبت به چگونگی عملکرد پایگاه‌داده و محل فایل‌ها و مصنوعات مختلف اطلاع داشت. لازم به ذکر است که جمع‌آوری مصنوعات و شواهد می‌تواند سبب تغییر در پایگاه‌داده شود، بنابراین پیش از استخراج اطلاعات از پایگاه‌داده یا خارج از پایگاه‌داده باید نسبت به این موضوع و پایدار یا ناپایدار بودن اطلاعات آگاهی پیدا کرد.

برای هر یک از رویدادهای غیرمجاز در سامانه پایگاه‌داده به هنگام بررسی جرم، جداولی برای ارائه مستندات لازم در نظر گرفته شده است که می‌بایست در طول فرآیند جرم‌شناسی به طور دقیق تکمیل و به مدیریت سازمان برای پیگیری‌های لازم و طرح دعوی ارائه گردد. جدول ۳۵، کلیه جداول اطلاعاتی مربوطه را به تصویر کشیده است.

جدول ۳۶: تهیه‌ی مستند از فرآیند جرم‌شناسی در پایگاه‌داده‌ی اوراکل

درج غیرمجاز در جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐	استفاده از قابلیت Flashback ☐	
توضیحات			
حذف غیرمجاز محتوای جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐	استفاده از قابلیت Flashback ☐	
توضیحات			
مشاهده غیرمجاز محتوای جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐

شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐	استفاده از قابلیت Flashback ☐	
توضیحات			
بروزرسانی غیرمجاز محتوای جدول			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐	ممیزی ریزدانه ☐	
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐		
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از LogMiner ☐		
توضیحات			
تغییر غیرمجاز شمای پایگاه‌داده			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	ممیزی یکپارچه ☐		
منابع رویدادنگاری	رویدادنگاری در فایل redo log ☐	رویدادنگاری در قابل DDL log ☐	
شیوه یا ابزار تحلیل	LogMiner برای استخراج رویدادهای موجود در فایل redo log ☐		
امکان ترمیم	استفاده از قابلیت Flashback ☐	آرشیو داده‌های Flashback ☐	استفاده از قابلیت RecycleBin ☐
توضیحات			
تلاش برای یافتن نام کاربری یا کلمه‌ی عبور			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	خط‌مشی ora_logon_failures ☐		
منابع رویدادنگاری	فاقد منبع رویدادنگاری است.		
شیوه یا ابزار تحلیل	استخراج محتوای unified_audit_trail همراه با کد بازگشتی ۱۰۱۷ ☐		

امکان ترمیم	قفل کردن نام کاربری دستی یا به صورت خودکار ☐		
توضیحات			
تلاش برای یافتن شناسه‌ی یکتای سیستم			
وقوع جرم	عدم وقوع ☐	وقوع خصمانه ☐	وقوع ناخواسته ☐
شیوه ممیزی	فاقد شیوه ممیزی است.		
منابع رویدادنگاری	فایل رویدادنگاری مربوط به شنونده‌ی پایگاه‌داده ☐		
شیوه یا ابزار تحلیل	فاقد شیوه یا ابزار تحلیل است.		
امکان ترمیم	عدم استفاده از کلمات و واژه‌های متداول به عنوان SID ☐		
توضیحات			

۸ منابع

[1]. DB audit and security 360, version 5.0, SoftTree Technologies, Inc.

[2]. http://www.dba-oracle.com

[3]. Al-Dhaqm, A., Razak, S.A., Othman, S.H., Nagdi, A. and Ali, A., 2016. A GENERIC DATABASE FORENSIC INVESTIGATION PROCESS MODEL. Jurnal Teknologi, 78.

[4]. R. Ramakrishnan and J. Gehrke. Database Management Systems (Third Edition). McGraw-Hill, Inc. New York, NY, USA, 2003.

[5]. G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report, DTR-T001-01 Final, Air Force Research Laboratory, Rome, New York, 2001.

[6]. https://docs.oracle.com

[7]. https://en.wikipedia.org/wiki/Transaction_log

[8]. J. Shital, Forensic Investigation for Database Tampering using Audit Logs, International Journal of Engineering Research & Technology (IJERT), Vol. 4 Issue 03, March 2015

[9]. K. Fowler, SQL Server database forensics, presented at the Black Hat USA Conference, 2007.

[10]. Fasan, O.M. and Olivier, M.S., 2012. On Dimensions of Reconstruction in Database Forensics. In WDFIA (pp. 97-106).

[11]. Al-Dhaqm, A., Razak, S.A., Othman, S.H., Nagdi, A. and Ali, A., 2016. A GENERIC DATABASE FORENSIC INVESTIGATION PROCESS MODEL. Jurnal Teknologi, 78.

[12]. https://solutioncenter.apexsql.com/recover-sql-server-database-using-only-a-transaction-log-file-ldf-and-old-backup-files/

[13]. H. Q. Beyers, "Database forensics: Investigating compromised database management systems", 2013.

[14]. Khanuja, H.K., Adane, D.S.: A Framework For Database Forensic Analysis. Published in Computer Science & Engineering: An International Journal (CSEIJ) 2(3) (2012)

[15]. Finnigan, P., *Oracle Incident Response and Forensics:* Preparing for and Responding to Data Breaches, 2018, Apress, Berkeley, CA.

[16]. https://dbatricksworld.com/ora-38707-media-recovery-is-not-enabled/

[17]. http://www.innovateus.net/science/what-forensics

[18]. R. Urbano, 2017, Oracle Database Administrator's Guide, 12c Release 2 (12.2)