## الملخص

مع استمرار التوسع الحاصل في الشبكات اصبحت من المسائل الهامة . لقد اصبح " فيض التخزين " من اكثر الاهداف الشائعة لمهاجمة الشبكات وعلى الجانب الاخر فأن كثيراً من تقنيات الكشف والوقاية قد تم تطويرها لتأمين الانظمة والشبكات والمعروفة بأنظمة كشف الاختراق .

تتناول الاطروحة المقدمة مشكلة "فيض التخزين" وتقترح نظام كشف اختراق هو عبارة عن دمج نظام كشف اختراق الشبكة ونظام كشف اختراق المضيف . صمم هذا النظام لكشف أي محاولة هجوم من نوع " فيض التخزين " تستخدم تقنية " استدعاء/ قفز مسجل" اعتماداً على استخدام مجموعة من عناوين الذاكرة المتوفرة لتعليمات الاستدعاء /القفز الخاصة بملفات مكتبات الربط الديناميكي المحملة واستخدامها كعناوين عودة تشير الى شفرة المهاجم الخبيثة والمستخدمة لانتهاك النظام يولد النظام المقترح ملفين للتواقيع احدهما خاص بنظام كشف اختراق المضيف تعتمد الة المراقبة والكشف في نظام كشف اختراق الشبكة على تقنية "المسح عند الوصول" لمسك أي ملف يحتوي على توقيع الهجوم وتسجيلها في ملف سجل . الى جانب ذلك فان الة المراقبة والكشف في نظام كشف اختراق المضيف تعتمد على نظام "snort " لكشف ومسك أي من رزم البيانات في مرور الشبكة والتي تحتوي على توقيع الهجوم وتسجيلها في ملف سجل اخر . تطبق الة التحليل مجموعة من العمليات الاحصائية ونظام تحليل مضبب على ملفات السجل من اجل انتاج مجموعة من التقارير على شكل صفحات ويب نوع PHP والتي تمثل مخرجات التحليل التي تعطي درجة خطورة هجوم " فيض التخزين ".