

الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 1945 - سيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbas



Master's Thesis

To obtain the diploma of Master's Degree

Field of Study: **Computer Science**

Specialization: **Computer Systems Engineering (ISI)**

Theme

Evolution of the Penetration Test Lifecycle

Presented by
Abderrauof Atsamnia
Ibrahim Senouci

Defended on: **June, 2026**
In front of the jury composed of

Dr. KHALDI Miloud
Dr. BABA-AHMED Manel
M MEGHNINE Islem
Dr. BENDELLA Mohamed Salih

President of the Jury
Thesis Supervisor
Co-Supervisor
Examiner

Academic Year: 2025/2026

Abstract

Penetration testing remains a fundamental practice for assessing the security posture of modern information systems. Traditional methodologies, such as the Penetration Testing Execution Standard (PTES), NIST SP 800-115, and the OWASP Web Security Testing Guide, provide structured phase-based approaches to security assessment. However, these frameworks were designed for relatively static environments and rely heavily on sequential workflows and manual execution, which limits their effectiveness in contemporary contexts characterized by large-scale, dynamic, and cloud-native infrastructures.

This thesis analyzes the evolution of the penetration testing lifecycle in response to these challenges. Through a critical review of existing methodologies and tools, several structural limitations are identified, including tool fragmentation, lack of data interoperability, high dependence on manual processes, and limited scalability. These limitations hinder the ability of current approaches to operate effectively in environments where assets change continuously and where large volumes of data must be processed and correlated.

In response, this work proposes an evolved penetration testing lifecycle model grounded in three core principles: continuous operation, structured data flow, and automation-first execution. The proposed model reorganizes the classical lifecycle into an iterative and integrated process composed of seven phases, including continuous reconnaissance, automated enumeration, validation and enrichment, vulnerability discovery, analysis and correlation, and continuous reporting. Unlike traditional approaches, the model emphasizes data normalization as a central component, enabling coherent aggregation and analysis of heterogeneous tool outputs.

The proposed lifecycle provides a conceptual framework that aligns penetration testing practices with modern paradigms such as DevSecOps and continuous security assessment. By addressing the limitations of existing methodologies and formalizing the integration between lifecycle phases, this work contributes to the development of more scalable, adaptive, and data-driven security testing processes.

Keywords penetration testing, lifecycle evolution, cybersecurity, automation, data normalization, DevSecOps

الملخص

يُعدّ اختبار الاختراق "Penetration Testing" ممارسةً أساسيةً لتقييم الوضع الأمني لأنظمة المعلومات الحديثة. تُقدّم المنهجيات التقليدية، كـ "Penetration Testing Execution Standard (PTES)"، و "NIST SP 800-115"، و "OWASP Web Security Testing Guide"، مقاربات منظّمة قائمةً على مراحل متتالية. غير أن هذه الأطر صُمّمت في الأصل لبيئات ثابتة نسبياً، وتعتمد اعتماداً كبيراً على سير العمل التسلسلي والتنفيذ اليدوي، مما يُحدّ من فعاليتها في السياقات المعاصرة التي تميّز بنى تحتية واسعة النطاق وديناميكية وقائمة على السحابة.

يُحلّل هذا المذكرة تطوّر دورة حياة اختبار الاختراق في مواجهة هذه التحديات. من خلال مراجعة نقدية للمنهجيات والأدوات القائمة، تم تحديد عدة قيود هيكلية، أبرزها: تشتت الأدوات، وغياب قابلية التشغيل البيئي للبيانات، والاعتماد الكبير على العمليات اليدوية، ومحدودية قابلية التوسع. تحول هذه القيود دون قدرة المقاربات الحالية على العمل بكفاءة في بيئات تتغيّر فيها الأصول باستمرار ويجب فيها معالجة كميات كبيرة من البيانات وربطها.

استجابةً لذلك، يقترح هذا العمل نموذجاً متطوراً لدورة حياة اختبار الاختراق، مبنياً على ثلاثة مبادئ جوهرية: التشغيل المستمر، وتنظيم تدفق البيانات، والتنفيذ القائم على الأتمتة. يُعيد النموذج المقترح تنظيم دورة الحياة الكلاسيكية في شكل عملية تكرارية متكاملة مؤلفة من سبع مراحل، تشمل: الاستطلاع المستمر، والتعداد الآلي، والتحقق والإثراء، واكتشاف الثغرات، والتحليل والترابط، والإعدادات التقييمية المستمر. وعلى خلاف المقاربات التقليدية، يُولي النموذج أهميةً محوريةً لتطبيع البيانات "Data Normalization"، مما يُتيح التجميع المتناسك وتحليل المخرجات غير المتجانسة للأدوات المختلفة.

يوفر النموذج المقترح إطاراً مفاهيمياً يُؤمّن ممارسات اختبار الاختراق مع النماذج الحديثة كـ "DevSecOps" والتقييم الأمني المستمر. من خلال معالجة قيود المنهجيات القائمة وتبني التكامل بين مراحل دورة الحياة، يُسهّم هذا العمل في تطوير عمليات اختبار أمنية أكثر قابليةً للتوسع والتكيف وقائمةً على البيانات.

الكلمات المفتاحية: اختبار الاختراق "Penetration Testing"، تطوّر دورة الحياة، الأمن السيبراني، الأتمتة "Automation"، تطبيع البيانات "Data Normalization"، "DevSecOps"

Résumé

Les tests d'intrusion constituent une pratique essentielle pour évaluer la posture de sécurité des systèmes d'information modernes. Les méthodologies traditionnelles, telles que le Penetration Testing Execution Standard (PTES), NIST SP 800-115 et l'OWASP Web Security Testing Guide, proposent des approches structurées basées sur des phases. Cependant, ces cadres ont été conçus pour des environnements relativement statiques et reposent fortement sur des processus séquentiels et manuels, ce qui limite leur efficacité dans des contextes modernes caractérisés par des infrastructures dynamiques, distribuées et orientées cloud.

Ce mémoire analyse l'évolution du cycle de vie des tests d'intrusion face à ces défis. À travers une étude critique des méthodologies et des outils existants, plusieurs limitations structurelles sont identifiées, notamment la fragmentation des outils, le manque d'interopérabilité des données, la forte dépendance aux processus manuels et les problèmes de passage à l'échelle.

Pour répondre à ces limites, ce travail propose un modèle évolué du cycle de vie des tests d'intrusion fondé sur trois principes fondamentaux : le fonctionnement continu, la structuration des flux de données et une approche orientée automatisation. Le modèle proposé réorganise le cycle de vie classique en un processus itératif composé de sept phases, incluant la reconnaissance continue, l'énumération automatisée, la validation et l'enrichissement, la découverte des vulnérabilités, l'analyse et la corrélation, ainsi que le reporting continu.

Ce modèle offre un cadre conceptuel permettant d'aligner les pratiques de test d'intrusion avec les paradigmes modernes tels que le DevSecOps et la sécurité continue. En adressant les limitations des approches existantes et en structurant l'intégration entre les différentes phases, ce travail contribue à l'évolution vers des processus de sécurité plus adaptatifs, scalables et orientés données.

Mots-clés test d'intrusion, évolution du cycle de vie, cybersécurité, automatisation, normalisation des données, DevSecOps