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 Abbes

Graduation Thesis

To obtain the diploma of **Engineering Degree**

Field of Study: **Computer Science**

Specialization: **Computer Systems Engineering**

Theme

Implementation of a Proxmox Backend for URSID: Automated Deployment of Cyber-ranges

---

Presented by
Malak BAZINE

Defended on: **September 17, 2025**
In front of the jury composed of

Dr. Hamdan BENSENANE	President of the Jury
Pr. Abdellatif RAHMOUN	Thesis Supervisor
Pr. Jean-François LALANDE	Co-Supervisor
Dr. Miloud KHALDI	Examiner

Academic Year: 2024/2025

Abstract

The exponential growth of cybersecurity threats, combined with a critical shortage of skilled professionals, has created an urgent need for effective hands-on training solutions. Traditional cybersecurity education methods fail to provide the realistic, scalable environments necessary for developing practical skills in defending against sophisticated attack scenarios. URSID (Using formalism to Refine attack Scenarios for vulnerable Infrastructure Deployment) addresses this challenge by automatically generating vulnerable network environments from formal attack scenario descriptions using the MITRE ATT&CK framework.

However, URSID's current backend architecture presents significant limitations that restrict its accessibility and adoption. The Vagrant backend supports only single-machine deployments, preventing realistic multi-system attack scenarios, while the OpenStack backend requires substantial infrastructure investment and operational expertise that creates barriers for smaller educational institutions.

This thesis presents the design and implementation of a Proxmox-based backend for URSID that bridges the gap between functionality and accessibility. The solution provides comprehensive multi-host virtualization capabilities without the operational complexity of cloud platforms, enabling educational institutions to deploy sophisticated cybersecurity training scenarios with moderate resource requirements and technical expertise.

The implementation follows a four-phase deployment lifecycle: initialization for environment preparation and resource discovery, deployment for virtual machine provisioning through template-based cloning, provisioning for scenario-specific configuration through Ansible automation, and cleanup for systematic infrastructure teardown. The backend integrates with URSID's existing scenario generation pipeline while leveraging Proxmox's unified API and management interface to minimize deployment complexity.

Validation through deployment of the BreizhCTF scenario demonstrates the backend's capability to handle realistic cybersecurity training challenges while maintaining compatibility with URSID's constraint resolution system. The implementation successfully addresses the identified limitations of existing backends, providing a balanced solution that combines advanced virtualization features with operational simplicity, thereby expanding URSID's potential adoption across diverse educational environments.

Keywords— Cybersecurity training, Virtualization, Cyber ranges, Automated deployment, URSID, Proxmox, MITRE ATT&CK, infrastructure as code, educational technology

Résumé

La croissance exponentielle des menaces de cybersécurité, combinée à une pénurie critique de professionnels qualifiés, a créé un besoin urgent de solutions de formation pratique efficaces. Les méthodes traditionnelles d'éducation en cybersécurité échouent à fournir les environnements réalistes et évolutifs nécessaires au développement de compétences pratiques pour se défendre contre des scénarios d'attaque sophistiqués. URSID (Using formalism to Refine attack Scenarios for vulnerable Infrastructure Deployment) répond à ce défi en générant automatiquement des environnements réseau vulnérables à partir de descriptions formelles de scénarios d'attaque utilisant le framework MITRE ATT&CK.

Cependant, l'architecture backend actuelle d'URSID présente des limitations significatives qui restreignent son accessibilité et son adoption. Le backend Vagrant ne supporte que les déploiements sur machine unique, empêchant les scénarios d'attaque multi-systèmes réalistes, tandis que le backend OpenStack nécessite des investissements infrastructurels substantiels et une expertise opérationnelle qui créent des barrières pour les plus petites institutions éducatives.

Cette thèse présente la conception et l'implémentation d'un backend basé sur Proxmox pour URSID qui comble le fossé entre fonctionnalité et accessibilité. La solution fournit des capacités de virtualisation multi-hôtes complètes sans la complexité opérationnelle des plateformes cloud, permettant aux institutions éducatives de déployer des scénarios de formation en cybersécurité sophistiqués avec des exigences modérées en ressources et expertise technique.

L'implémentation suit un cycle de vie de déploiement en quatre phases : initialisation pour la préparation de l'environnement et la découverte des ressources, déploiement pour l'approvisionnement de machines virtuelles par clonage basé sur des modèles, provisioning pour la configuration spécifique aux scénarios par automatisation Ansible, et nettoyage pour le démantèlement systématique de l'infrastructure. Le backend s'intègre avec le pipeline de génération de scénarios existant d'URSID tout en exploitant l'API unifiée et l'interface de gestion de Proxmox pour minimiser la complexité de déploiement.

La validation à travers le déploiement du scénario BreizhCTF démontre la capacité du backend à gérer des défis de formation en cybersécurité réalistes tout en maintenant la compatibilité avec le système de résolution de contraintes d'URSID. L'implémentation répond avec succès aux limitations identifiées des backends existants, fournissant une solution équilibrée qui combine des fonctionnalités de virtualisation avancées avec une simplicité opérationnelle, élargissant ainsi le potentiel d'adoption d'URSID à travers divers environnements éducatifs.

Keywords— Formation en cybersécurité, Virtualisation, Cyber ranges, Déploiement automatisé, URSID, Proxmox, MITRE ATT&CK, infrastructure as code, technologie éducative

الملخص

أدى النمو الهائل في تهديدات الأمن السيبراني، مقترناً بنقص حاد في المهنيين المهرة، إلى خلق حاجة ملحة لحلول التدريب العملي الفعالة.
تفشل أساليب تعليم الأمن السيبراني التقليدية في توفير البيئات الواقعية والقابلة للتوسع الضرورية لتطوير المهارات العملية للدفاع ضد سيناريوهات الهجمات المتطورة. يعالج نظام (استخدام الصياغة الرسمية لتحسين سيناريوهات الهجمات لنشر البنية التحتية الضعيفة) هذا التحدي من خلال إنتاج بيئات شبكية ضعيفة تلقائياً من أوصاف سيناريوهات الهجمات الرسمية باستخدام إطار عمل .
ومع ذلك، تقدم هندسة الواجهة الخلفية الحالية لنظام قيوداً كبيرة تحد من إمكانية الوصول إليه واعتماده. تدعم واجهة الخلفية فقط عمليات النشر على آلة واحدة، مما يمنع سيناريوهات الهجمات متعددة الأنظمة الواقعية، بينما تتطلب واجهة kcatSnepO الخلفية استثمارات بنية تحتية كبيرة وخبرة تشغيلية تخلق حواجز للمؤسسات التعليمية الصغيرة.
تقدم هذه الأطروحة تصميم وتنفيذ واجهة خلفية قائمة على xomxorP لنظام DISRU تسد الفجوة بين الوظائف وإمكانية الوصول. يوفر الحل قدرات محاكاة افتراضية متعددة المضيفين شاملة دون التعقيد التشغيلي للمنصات السحابية، مما يمكن المؤسسات التعليمية من نشر سيناريوهات تدريب أمن سيبراني متطورة بمتطلبات موارد وخبرة تقنية معتدلة.
يتبع التنفيذ دورة حياة نشر من أربع مراحل: التهيئة لإعداد البيئة واكتشاف الموارد، والنشر لتوفير الآلات الافتراضية من خلال الاستنساخ القائم على القوالب، والتحضير للتكوين الخاص بالسيناريو من خلال أتمتة ، والتنظيف للهدم المنهجي للبنية التحتية. تتكامل الواجهة الخلفية مع خط أنابيب توليد السيناريوهات الموجود في بينما تستفيد من واجهة برمجة التطبيقات الموحدة وواجهة إدارة لتقليل تعقيد النشر.
يُظهر التحقق من خلال نشر سيناريو قدرة الواجهة الخلفية على التعامل مع تحديات التدريب على الأمن السيبراني الواقعية مع الحفاظ على التوافق مع نظام حل القيود في . ينجح التنفيذ في معالجة القيود المحددة للواجهات الخلفية الموجودة، مما يوفر حلاً متوازناً يجمع بين ميزات المحاكاة الافتراضية المتقدمة والبساطة التشغيلية، وبالتالي توسيع إمكانات اعتماد عبر بيئات تعليمية متنوعة.

الكلمات المفتاحية--- تدريب الأمن السيبراني، المحاكاة الافتراضية، نطاقات الأمن السيبراني، النشر الآلي، البنية التحتية كرمز، التكنولوجيا التعليمية