Automated Cyber Range Infrastructures for Securing Tomorrow: Lessons from Range42

Abstract

The future of cyber conflict demands training and testing platforms that anticipate tomorrow's threats rather than replicate yesterday's incidents. This paper presents Range42, an open cyber range developed by the National Cybersecurity Competence Center (NC3) under the Luxembourg House of Cybersecurity together with DIGISQUAD. Designed as a flexible, automated platform, Range42 lowers barriers to building realistic and reproducible training environments while fostering collaborative research and development.

Our research introduces two core contributions. First, we describe an extensible inventory system of vulnerable and misconfigured environments. With over 100 curated CVEs and misconfigurations identified and approximately 20 already deployable, this system enables structured reproduction of real-world attack surfaces for controlled experiments. Second, we detail an orchestration framework capable of deploying multi-subnet infrastructures, making it possible to simulate complex enterprise-grade networks with isolation and fidelity.

We outline the automation pipeline—including Proxmox integration, Ansible-driven provisioning, container and VM deployment, and Tailscale-enabled zero-trust connectivity—and assess its ability to create scalable, reusable, and secure scenarios.

We conclude that open, automated cyber ranges such as Range42 are essential to "securing tomorrow." They enable hands-on training, accelerate scenario design, and provide accessible platforms for testing defensive strategies against emerging threats.

Introduction

Cyber threats evolve faster than training and evaluation methodologies. To secure tomorrow, cyber ranges must enable realistic, reproducible, and rapidly composed environments that reflect emerging attack surfaces and defensive strategies. We present Range42, an open cyber range platform emphasizing automation, flexibility, and collaboration. Our contributions are: (1) an extensible inventory of vulnerable/misconfigured systems for research-grade reproducibility; and (2) an orchestration framework for deploying multi-subnet infrastructures approximating enterprise topologies. We outline our automation pipeline and report lessons for scalability, isolation, and openness.

Background and Related Work

Prior work spans commercial, academic, and government cyber ranges; however, many platforms are closed or bespoke, limiting reproducibility, comparability, and community validation. Open, automated ranges reduce barriers for training, experimentation, and replication of results. We position Range42 in this landscape and identify gaps in open orchestration, inventory standardization, and zero-trust access for distributed exercises.

System Architecture

Range42 integrates: (i) Proxmox for VM lifecycle; (ii) Ansible for idempotent provisioning; (iii) containers and VMs for workload flexibility; and (iv) Tailscale (WireGuard-based) for identity-aware, zero-trust connectivity. Figure 1 sketches the build–deploy–run pipeline and control surfaces.

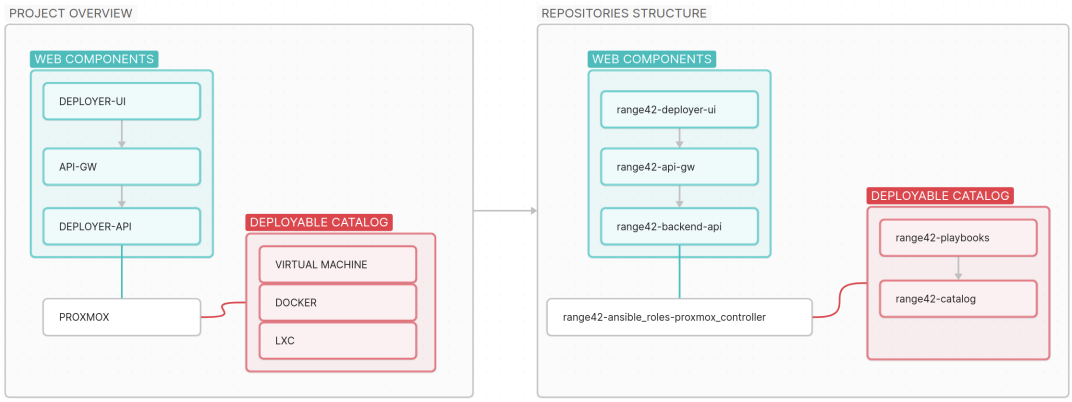

Figure 1: High-level Range42 architecture and automation pipeline (placeholder).

Vulnerability and Misconfiguration Inventory

We curate an inventory of ∼100 CVEs/misconfigurations (with ∼20 currently deployable), using build descriptors and snapshotting to balance reproducibility with support for proprietary or atypical systems. The design supports traceability, variant creation, and controlled risk exposure during exercises.

Multi-Subnet Orchestration

Realistic exercises require routed, segmented networks. Our orchestration composes multi-subnet topologies with per-segment policy, enabling blue/red/purple-team exercises and layered defenses. We discuss challenges (addressing, routing, firewall policy, performance) and our mitigation strategies using Proxmox APIs and Ansible roles.

Evaluation

We evaluate deployment time, reproducibility, and scale (concurrent labs/users) across representative scenarios. Where quantitative metrics are constrained by resource ceilings, we complement with qualitative feedback from instructors and operators. We report failure modes and remedies observed during pilot training events.

Discussion

We reflect on security trade-offs (fidelity vs. containment), operational debt (image sprawl, secret handling), and governance (open contributions, quality gates). We argue that openness is a force multiplier for resilience: it improves scrutiny, reuse, and portability across institutions.

Future Work

Planned work includes: expanding inventory coverage; advancing a visual lab designer; integrating malware analysis/forensics workflows; and supporting richer hybrid topologies. We also plan a unified scenario descriptor (YAML/JSON) to drive the gateway/orchestrator for end-to-end reproducibility.

Conclusion

Open, automated ranges like Range42 help secure tomorrow by enabling hands-on research and training at scale. Our contributions—a reproducible inventory and multi-subnet orchestration—demonstrate a practical path to scalable, high-fidelity, and community-driven cyber range operations.

References

[1] Proxmox VE. Available: https://www.proxmox.com/

[2] Ansible Documentation. Available: https://docs.ansible.com/

[3] Docker Documentation. Available: https://docs.docker.com/

[4] Tailscale Documentation. Available: https://tailscale.com/kb/

[5] IEEE Editorial Style Manual. Available: https://journals.ieeeauthorcenter.ieee.org/