GPU-Accelerated Password Auditing — Summary

Author: Velkris (Jared Perry)
Focus: Red Team Infrastructure / Password Auditing & Cracking Optimization
Environment: Controlled GPU-accelerated lab (Windows host + NVIDIA RTX 3080)
Purpose: Validate and benchmark GPU-based password cracking workflows for efficiency, reproducibility, and red-team exercise realism.

Objective

Configure and benchmark a GPU-based password auditing environment to compare CPU vs GPU cracking performance across common hash types (NTLM, MD5, SHA1), ensuring reliable baselines for red-team and training simulations.

Lab Setup

Component	Details
Hardware	NVIDIA RTX 3080 (CUDA 12.x) with 10GB VRAM
Software	Hashcat 6.x, Windows Subsystem for Linux (WSL2), NVIDIA drivers (550+)
Test Hashes	NTLM, MD5, SHA1, bcrypt (controlled test datasets)
Wordlists	RockYou, CrackStation, custom hybrid rulesets

Methodology

- Configured GPU acceleration with Hashcat (CUDA backend) and validated device recognition.
- Conducted comparative benchmarks between CPU-only and GPU-based cracking sessions.
- Measured hash-per-second (H/s) throughput across different modes and keyspaces.
- Documented environment variables, kernel tuning, and workload balancing configurations.

Observations

Category	Finding
Performance Gain	Average ~4× improvement in cracking throughput over CPU-only tests.
Stability	Sustained load at 98% GPU utilization for >3 hours with thermal control <70°C.
Script Efficiency	Automated benchmarking scripts reduced test setup time by 50%.

Tools & Scripts

Hashcat • CUDA Toolkit • Hashcat-utils • Python benchmarking script • Custom PowerShell automation for hash-type sequencing

---

Key Takeaways

- GPU acceleration provides significant performance uplift for password audit workflows.
- Automation enables **repeatable and measurable** cracking benchmarks for red-team readiness.
- Controlled datasets ensure ethical, lab-only use compliant with internal testing policies.

Outcome

Delivered a **validated GPU cracking benchmark suite** integrated into red-team exercise planning and lab readiness checks.
Improved lab throughput and shortened password audit timelines, enhancing operational realism for adversary-simulation engagements.

> This project demonstrates both technical depth in GPU optimization and disciplined operational methodology under controlled, ethical testing environments.