The Overclock Experience

<HACK/NET™>

HEURISTICS ACCELERATING CYBER KNOWLEDGE NETWORK

Living and learning in the modern cybersecurity residence hall

BACKGROUND

Hands-on learning is essential in cybersecurity because threats and technologies evolve faster than theory alone can cover. Labs, ranges, competitions, and projects outside the classroom allow students to build applied skills and grow their confidence.

PROBLEM

Many cybersecurity programs emphasize lectures and theory, leaving students underprepared for the fast-changing, hands-on nature of real-world threats. Without experiential learning, graduates lack the skills employers need for immediate workforce readiness.

SOLUTION

We created an immersive cybersecurity experience that combines classroom learning, 24/7 living, and an on-demand cyber range where students learn in a cyber-focused community. The approach blends engagement with real-world practice to prepare students for the workforce.

Bridging the Gap Between the Classroom and Operations

24/7 Access: Learning doesn't stop at the classroom door.

Immersive Environment: Integrated directly into student residence hall.

Experimental Learning: Real-world threat landscapes and cross-disciplinary collaboration.

ECOSYSTEM

Enhance Workforce Readiness
Ensure students graduate with practical, industry-aligned skills gained through labs, ranges, competitions, and client projects.

Build a Learning Community
Provide a 24/7 environment where students live, collaborate, and problem-solve together, strengthening retention and mentoring.

Industry-Standard Tooling
The network is equipped with professional security monitoring and incident response tools, ensuring that the practical experience directly translates to the technical realities of the modern cybersecurity field.

Ethics and Safety
Every participant must sign a rigorous AUP, defining the clear boundaries between sanctioned research and prohibited activity. All HACKnet activities are governed by the University's code of conduct.

Additional Opportunities
Create assessments via surveys, usage metrics, set learning outcome objectives which to measure.
By expanding our server capacity and deploying a wider variety of virtual targets, we're creating a robust sandbox for students to test their skills against the latest vulnerabilities.

HACKNet Architecture

Tiered Network Design for Progressive Skill Development

Level	Environment Type	Security Landscape
Easy	Vulnerable Web Apps	Entry-level hackable targets for foundational practice
Medium	Corporate Infrastructure	Lax security controls and patching
Hard	Enterprise Infrastructure	Stringent security controls and frequent patching

Gamified Skill Building

Capture the Flag (CTF) Methodology

Sophisticated Exploits: Higher complexity breaches yield greater point rewards.

Strategic Thinking: Fosters systematic analysis through 'learning by doing'.

Risk-Free Offensive Training: CTFs provide a "legal playground" where students can perform aggressive network scanning and penetration testing.

David Richards
Executive Director

Grand Canyon University
Cyber Center of Excellence

David.Richards@gcu.edu

GRAND CANYON UNIVERSITY®