Cole A. Ellis

ECHOCOLEELLIS@GMAIL.COM · COLE-ELLIS.COM · GITHUB.COM/THECAE

PROFESSIONAL WORK EXPERIENCE

National Cyber Protection Team 81, USCYBERCOM *Splunk, VMWare — Defensive Cyberspace Operations*

- Aided in the infrastructure and engineering of a Cyber Defense Kit used on a Hunt Forward Operation.
- Performed research on the current threat landscape, emerging cyber threats, and adversarial tactics and procedures and applied findings to the improvement of the Cyber Defense Kit.
- Used commercial, off-the-shelf software including the VMware suite to manage virtual machines, the Carbon Black suite to **monitor network traffic** and **detect malicious activity**, and the Splunk suite to aggregate and analyze logs.
- Assisted in the development of a local network matching customer network architecture to perform pre-deployment testing.

Naval Cyber Warfare Engineer Cruise *C, Python, ARM & x86 Assembly — Penetration Testing*

- Collaborated within a team of five Midshipmen to prevent a simulated missile launch through **successful system penetration**.
- Exploited Java deserialization vulnerability and performed Docker escape to **gain root access** to the server.
- Utilized an undersized RSA key crack to sign a custom DLL, enabling decryption of chat logs and real-time traffic observation on a Rocket.Chat derivative.
- Achieved Remote Code Execution via buffer overflow exploitation in an ARM binary using ret2plt, and subsequently **developed a Remote Access Trojan (RAT)** and rootkit to halt the missile launch without being detected.

Escape Room Design *Python, Assembly, SQL, HTML — Full Stack Development*

- **Engineered three operational escape rooms**, integrating custom software and hardware for an immersive user experience.
- Developed a backend using Python to manage game flow; incorporated Arduino, Raspberry Pi, and Intel DE10 FPGA circuits for game logic, mechanics, and visual/special effects.
- Utilized MySQL for a robust record management system and HTML for user-facing web interfaces.
- Implemented accessible interfaces for administrators to effortlessly modify gameplay and backend operations.

Intermediate Software Design (CS-3251) Teaching Assistant *C++ — Teaching and Code Review*

- Graded programming assignments, held office hours, and aided in the instruction of 150 students.

PROJECTS

DARPA CASTLE Research Participant *Python — Cybersecurity, Artificial Intelligence, Machine Learning*

- Aided in the development of **autonomous offensive and defensive network agents** to infiltrate and defend networks.
- Leveraged Velociraptor, CybORG, and RLLib libraries to rapidly develop testing models.
- Automated the deployment of testing environments to replicate real-world scenarios and test and train agents.
- Created a web-based dashboard to demonstrate the performance of each agent and areas for improvement.

VUNROTC CWE Preparation Course *C, ASM, Python — Cybersecurity Education*

- Conceived and **single-handedly developed** a comprehensive, CTF-style course to equip Midshipmen with requisite skills for the Cyber Warfare Engineering accessions screener.
- Invested significant time in **creating over 50 unique, graded challenges** with varying levels of security to train students in binary overflow techniques, C programming for problem-solving, and reverse engineering.
- Conducted intensive, twice-weekly educational sessions focusing on essential cybersecurity skills tested in the CWE screener.

EDUCATION

School of Engineering, Vanderbilt University, Nashville, TN
"14th in Best Colleges and Universities" - U.S. News and World Report
B.S. Computer Science

- GPA: 3.34, Major GPA: 3.62
- *Coursework*: Data Protection & Cybersecurity, Reverse Engineering, Operating Systems, Software Design, Databases, Data Structures & Algorithms, Intermediate Chinese, Leadership & Ethics, Leadership & Management
- *Activities*: Vanderbilt CTF, VandyHacks, Vanderbilt NROTC, Ultimate Frisbee, VandyLifts

SKILLS

- *Languages*: C, C++, Python, Java, PHP, SQL, HTML/CSS/JS, Swift, LaTeX
- *Applications*: Ghidra, Burpsuite, Wireshark, Radare2, GDB, Docker, Splunk, Git, VScode
- *Operating Systems*: Ubuntu Linux, Kali Linux, Windows, MacOS
- *Virtual Systems*: VMWare Workstation, VMWare Horizon, vSphere, VMWare Carbon Black, pfSense
- Proficient in Spanish (oral and written), moderate fluency in Mandarin Chinese (oral and written).