Final Project: Technical Exploitation and Societal Security

Bowie State University
Department of Computer Science
Devharsh Trivedi, Ph.D., CISSP
Spring 2026

1 Project Overview

Students will form collaborative teams consisting of two to three members to conceptualize, design, implement, and critically evaluate a cybersecurity solution, technical tool, or controlled exploit. Each team is expected to demonstrate not only technical proficiency but also analytical depth by examining the broader societal, ethical, legal, and policy implications associated with their chosen project. Emphasis should be placed on understanding how technical security mechanisms influence individuals, organizations, and society at large, including privacy, trust, risk, governance, and responsible use.

This assignment intentionally bridges the hands-on offensive and defensive security methodologies emphasized in COSC 489: Ethical Hacking with the interdisciplinary perspective of COSC 442: Cybersecurity and Society. Students are required to apply advanced technical concepts, such as vulnerability analysis, exploitation, detection, and mitigation, while engaging with questions of ethics, public policy, social impact, and professional responsibility.

The project is structured around a formal 16-week scholarly research and development lifecycle that mirrors real-world academic and industry practices. Throughout the semester, teams will progress through topic selection, proposal development, literature review, methodological design, implementation, evaluation, and dissemination. The project culminates in the completion and submission of the following required deliverables:

- A professional scholarly manuscript of 20 or more pages, single-spaced, with a plagiarism similarity score below 20 percent
- A formal preprint publication with a Digital Object Identifier
- A live technical demonstration of a functional proof of concept conducted in Kali Linux
- A public GitHub repository demonstrating professional software engineering practices and contributions from all team members

All technical work must be conducted ethically and strictly within controlled and authorized environments.

2 Research Tracks and Project Ideas

Teams may select a project from the approved list provided below or develop an original project idea aligned with the course objectives. Any proposed custom topic must be submitted for review and receive the instructor's explicit approval before work may begin.

2.1 Track 1: Advanced Research, Innovation, and Privacy Preserving Systems

- AI-Powered Offensive Cybersecurity Agent for Capture the Flag competitions
- Hybrid privacy preserving analytics using Fully Homomorphic Encryption and Secure Multi-Party Computation
- Fully Homomorphic Encryption in distributed tax or audit systems
- Split learning architectures for on-device privacy protection
- Deepfake detection using polynomial approximation of facial micro expressions
- Comparative evaluation of post-quantum cryptography schemes
- Automated malware attribution using large language model embeddings and graph neural networks
- Adaptive deep learning systems for real-time fraud detection
- Dynamic risk management for third party and supply chain vulnerabilities
- Zero Trust Architecture migration and enterprise design

2.2 Track 2: Autonomous Threats, AI Security, and Offensive Simulations

- Agentic artificial intelligence for offensive Capture the Flag challenges
- Automated deepfake detection logic using nonlinear modeling
- Modern phishing simulation and human risk analysis
- Adversary emulation and detection engineering using MITRE ATT&CK

2.3 Track 3: Specialized Technical Tools and Ethical Hacking

- Simplified mobile API vulnerability scanner for Broken Access Control and IDOR
- Mobile application vulnerability analysis using Frida or mitmproxy
- Automated web application fuzzer

- Network protocol analyzer and packet sniffer
- Wi Fi security auditing tool for authorized hardware only
- Hardware security analysis of embedded systems using firmware extraction
- Ethical exploit development proof of concept using buffer overflows
- Exploit development framework for controlled environments
- Cloud security auditing using Infrastructure as Code scanners
- Container security scanner for Docker images
- Lightweight SIEM development
- Digital forensics and incident response playbook for ransomware scenarios

3 Sixteen Week Research and Development Timeline

Week	Phase	Activities and Deliverables
1	Initiation	Team formation and topic selection
2 to 3	Proposal	Submission of one page proposal including title team abstract and keywords
4 to 5	Literature Review	Review and synthesis of at least 20 peer-reviewed scholarly sources
6 to 8	Methods	Technical methodology design and Kali Linux lab setup
9 to 11	Implementation	Code development and ethical testing in controlled environments
12 to 14	Drafting	Final data analysis and writing of 20-plus-page single-spaced paper
15	Publication	Submission to preprint server and DOI acquisition
16	Live Demonstration	Live technical demonstration and presentation in Kali Linux

4 Technical and GitHub Submission Standards

Each team must maintain a public GitHub repository demonstrating professional software engineering practices and meaningful contributions from all members.

Required repository components include:

- /src directory with modular commented source code and proper error handling
- /docs directory containing the project report, user manual, and DOI link

- /tests directory with unit tests, integration tests, and sample logs
- README file with setup instructions, usage examples, and ethical considerations
- requirements file listing all dependencies
- .gitignore file excluding build artifacts and sensitive data

5 Ethical Mandate

All experimentation must be conducted exclusively in controlled environments such as virtual machines, test networks, or explicitly authorized systems. Unauthorized scanning, exploitation, or testing of live systems is strictly prohibited and will result in a failing grade. Each project must include a dedicated section addressing ethical considerations, responsible use limitations, and safeguards against misuse.

6 Approved Preprint Servers for DOI Generation

By Week 15, teams must submit their final manuscript to one of the following platforms:

- Zenodo `https://zenodo.org`
- Preprints.org `https://www.preprints.org`
- ResearchGate `https://www.researchgate.net`
- arXiv `https://arxiv.org`
- TechRxiv `https://www.techrxiv.org`

7 Final Note

This assignment constitutes the complete and final specification for the joint COSC 489 and COSC 442 final project. It integrates advanced technical exploitation, ethical hacking practices, cybersecurity policy analysis, and formal scholarly publication standards into a single unified capstone experience.