Proposed Penetration Testing Course and Curriculum Alignment for UNF Cybersecurity Preparation

Developed from Directed Independent Study Deliverables 1 and 2 and formatted in the general style of the CNT 4504 syllabus provided by the user.

Institution	University of North Florida
Proposed course shell	CIS 4930 Special Topics: Penetration Testing and Adversary Emulation Short-term pilot shell before permanent SCNS numbering
Prepared for	Directed Independent Study Deliverable 3

Executive Summary

This proposal converts the findings from the as-is and to-be analyses into a practical academic recommendation for UNF. The core finding across both deliverables is that the team is underprepared not because students lack motivation, but because training is too infrequent, too lab-centric, too weakly aligned with real competition conditions, and too dependent on a small number of competition-ready members.

A new upper-level penetration testing course is recommended as part of the solution. The course is not intended to teach students how to attack for its own sake. Instead, it uses controlled adversarial techniques to strengthen defensive understanding, improve triage and prioritization, build familiarity with enterprise attack paths, and create a more realistic bridge between lecture content and competition conditions.

The proposal recommends a near-term pilot using a Special Topics shell, followed by a permanent catalog course after faculty review. It also recommends targeted changes to existing computing courses so that penetration testing material complements, rather than replaces, UNF's existing security sequence.

Why this course is justified by the research

- Deliverable 1 found that mock competitions and tabletop exercises were effectively absent, while guided labs and independent labs dominated preparation.
- Deliverable 1 also found that readiness was concentrated in a small core, with respondents reporting that only one or two people were often truly competition-ready before events.
- Deliverable 2 concluded that stronger performance requires repeated simulation, clearer role execution, more realistic scenarios, better documentation habits, and stronger integration of injects, reporting, triage, and recovery.

Part I - Proposed Course Syllabus

CIS 4930 Special Topics: Penetration Testing and Adversary Emulation

Course Type	Upper-level undergraduate cybersecurity elective / special topics pilot
Credits	3
Recommended Placement	Junior or senior level in the Information Technology curriculum
Proposed Prefix and Number	CIS 4930 in the short term; permanent CIS 43XX or CIS 46XX recommended after approval
Prerequisites	CIS 4360 Intro to Computer Security, CNT 4504 Computer Networks, and either CIS 4325 Intro to Sys Admin or instructor permission

Course Overview

This course gives students an opportunity to study penetration testing as a disciplined, authorized, and evidence-driven process that supports defense rather than replacing it. Topics include scoping and rules of engagement, reconnaissance, enumeration, vulnerability validation, privilege escalation concepts, Active Directory attack paths, web and service testing, pivoting, reporting, and remediation-oriented communication.

The proposed delivery model is lecture, guided lab, timed practical exercises, and controlled team-based scenarios.

Catalog description: Controlled study of penetration testing methods, adversary emulation, enumeration, exploitation validation, reporting, and defensive translation in enterprise environments. Emphasis is placed on authorization, scope control, evidence quality, communication, and using offensive understanding to improve system defense.

Course purpose: Build offensive literacy in a controlled setting so students can better secure, monitor, triage, and recover enterprise systems and competition environments.

The course is intentionally aligned with the weaknesses identified in the directed study. It emphasizes realistic workflow, timed exercises, documentation, role clarity, and communication under pressure. It is designed to support both academic preparation and defensive competition readiness.

Student Learning Outcomes

- Explain the legal, ethical, and procedural boundaries of authorized penetration testing.
- Perform reconnaissance, enumeration, and vulnerability validation against controlled targets.
- Demonstrate structured note taking, evidence collection, and change discipline during offensive testing.
- Identify common enterprise attack paths, especially those involving Windows administration, Active Directory, network exposure, and service misconfiguration.
- Translate offensive findings into defensive recommendations, prioritization, and remediation guidance.
- Produce professional technical and executive-facing penetration test reports.
- Operate effectively in timed practical exercises that require triage, communication, and team coordination.

Tentative Topic Schedule

Week	Module	Representative Topics / Activities
1	Authorized penetration testing	Scope, rules of engagement,

	foundations	ethics, reporting chain, lab safety, evidence handling
2	Reconnaissance and enumeration	Asset discovery, service fingerprinting, DNS and web enumeration, attack-surface mapping
3	Vulnerability analysis and validation	False positives vs. exploitable findings, severity, exploitability, and defensive meaning
4	Windows and enterprise attack paths	Authentication, privilege abuse concepts, AD exposure, hardening implications
5	Linux and service exploitation concepts	Misconfiguration discovery, service abuse paths, defensive translation
6	Web application testing basics	Common validation workflow, authentication flaws, input handling, report-quality proof
7	Network exploitation concepts	Segmentation testing, exposed services, firewall rule mistakes, pivoting concepts
8	Credential attacks and privilege escalation	Password spraying concepts, local escalation paths, secure handling and controls
9	Detection-aware testing	How offensive actions appear in logs, SIEM, EDR, and admin workflows
10	Reporting and remediation	Technical writing, executive summaries, risk ranking, reproducibility, remediation planning
11	Team exercise I	Timed testing block with notes, change discipline, and interim briefing
12	Team exercise II	Adversary emulation and defensive handoff

Representative Assignments and Grading

Assignment Category	Weight
Weekly labs and short skill checks	20%
Reconnaissance / enumeration practical	15%
Technical reporting assignment	15%
Midterm controlled assessment	20%
Team scenario exercise	10%
Final penetration test report and presentation	20%

Required Environment and Safety Expectations

- All technical exercises must be conducted only in instructor-approved lab environments or isolated virtual machines.
- No student may scan, exploit, or enumerate systems outside the explicit course scope.
- Tools are taught as instruments for validation, documentation, and defensive improvement.
- Students must preserve notes, timestamps, commands, and evidence sufficient to justify findings.

Worthy of Note

1. This course should include a clear authorization statement in the syllabus and on every lab handout.

2. Because the proposed course supports both academic learning and cyber competition readiness, the lab design should favor repeatable enterprise scenarios rather than one-off demonstrations.

3. If UNF prefers a more conservative launch path, the course can first run as a special topics offering before a permanent catalog number is requested.

Part II - Recommended Changes to Existing Courses

The new course should not stand alone. The study findings suggest that a single penetration testing course will be most effective if it is paired with narrower revisions to existing coursework so that enterprise defense, systems administration, detection, documentation, and competition workflow reinforce each other.

CIS 4360 - Intro to Computer Security

Current role: Foundation security course

Recommended action: Change

Reason based on study: Add stronger enterprise baseline coverage: Windows triage, Active Directory fundamentals, change logging, and first-hour hardening workflow.

CIS 4325 - Intro to Sys Admin

Current role: Systems administration course

Recommended action: Change

Reason based on study: Add service restoration drills, rollback discipline, and timed admin tasks because the study found weak recovery and self-inflicted outages.

CNT 4406 - Network Security / Management

Current role: Networking and security course

Recommended action: Change

Reason based on study: Add segmentation and firewall troubleshooting labs that mirror competition pressure and shared critical-asset priorities.

CIS 4364 - Intrusion Detection

Current role: Detection and monitoring course

Recommended action: Change

Reason based on study: Expand with attacker-technique-to-detection mapping so students see how penetration test actions surface in logs, SIEM, and host monitoring.

CIS 4366 - Computer Forensics

Current role: Evidence and investigation course

Recommended action: Change

Reason based on study: Add rapid evidence preservation during live incidents so technical fires do not eliminate reporting quality or investigative value.

CIS 4930 / new permanent CIS 43XX

Current role: Proposed penetration testing course

Recommended action: Add

Reason based on study: Provide the missing offensive literacy and controlled adversary practice that current coursework does not appear to cover directly.

No current course

Current role: N/A

Recommended action: Remove

Reason based on study: No existing security course should be removed outright. The stronger recommendation is selective revision plus one added course.

Specific add / change / remove recommendation

Add: one upper-level penetration testing course, first as CIS 4930 Special Topics and later as a permanent catalog course after UNF and SCNS approval.

Change: existing security, networking, and administration courses so they include more enterprise workflow, timed scenarios, documentation, and role-based exercises.

Remove: no current course needs to be deleted based on the study evidence. The problem identified by the research is not excessive security coursework. It is an alignment gap between existing coursework, competition conditions, and operational readiness.

Implementation Path

1. Pilot the course under a special topics shell so content, labs, and prerequisites can be tested quickly.

2. Collect assessment data from student performance, lab completion, reporting quality, and faculty observation.

3. Refine the course and request a permanent course number through the normal university and Florida course-numbering process.

4. Use the pilot results to determine whether the course should become an IT major elective, a cybersecurity track requirement, or both.

Part III - Notes on Florida Course Numbering Use

UNF uses Florida's Statewide Course Numbering System, so the final permanent number for a new course should be coordinated through the university approval process rather than assumed in advance.

For that reason, this proposal uses a conservative two-stage approach: first offer the course as CIS 4930 Special Topics, then assign a permanent upper-level CIS number after approval.

The CIS prefix is the best fit for the proposed course because the content centers on information security practice, enterprise systems, technical workflow, and defensive translation rather than pure networking alone.

Appendix - Mapping to Research Findings

Research finding	Syllabus / curriculum response
Mock competitions and tabletop work were rare or absent.	The proposed course includes timed practicals, team exercises, interim briefings, and reporting deliverables.
Readiness was concentrated in a small core.	The course creates a repeatable pipeline that gives more students direct exposure to realistic

Windows / Active Directory, Linux triage, inject handling, and reporting were undertrained.

Competition performance suffered from weak documentation, triage, and change control.

The to-be analysis recommended simulation, role clarity, and stronger workflow discipline.

adversary workflow.

The course topics and the recommended changes to CIS 4360, CIS 4325, CNT 4406, and CIS 4364 directly target those gaps.

Labs and assessments require evidence quality, note taking, rollback discipline, and remediation-oriented reporting.

The proposed syllabus is intentionally operational, scenario-based, and communication-heavy rather than lecture-only.

Appendix B - Recommended Texts, Open Materials, and Weekly Resource Map

The proposed course should not rely on a single exam-prep textbook. A better fit for UNF is a layered materials model: one assessment-process guide, one web-testing reference, one adversary-behavior reference, platform-specific administration and identity resources, and instructor-authored lab packets. This approach fits the study findings because the gap was operational readiness and workflow discipline, not a lack of disconnected tool exposure.

Recommended baseline resources:

• NIST SP 800-115 as the anchor for test planning, assessment structure, and mitigation-oriented reporting.

• PTES as the practical workflow reference for pre-engagement, intelligence gathering, validation, exploitation phases, and reporting.

• OWASP Web Security Testing Guide as the primary open guide for web testing modules and checklists.

• MITRE ATT&CK as the enterprise behavior model for mapping techniques to defensive observations and mitigations.

• Microsoft Learn and Windows Server identity/security documentation for Active Directory, Windows administration, and privilege-management background.

• Kali and Linux tool documentation as a reference source for supported tools and syntax, rather than as the course backbone.

• OWASP Juice Shop and picoCTF as legal hands-on practice environments for selected modules and optional enrichment.

• OpenSecurityTraining2 as optional depth material for binary, exploitation, or advanced enrichment topics.

Weekly resource mapping

Week	Module	Primary recommended resources	How the resource should be used
1	Authorized penetration testing foundations	NIST SP 800-115; PTES Pre-engagement	Define scope, rules of engagement, evidence expectations, and reporting structure before technical work begins.
2	Reconnaissance and enumeration	PTES Intelligence Gathering; Kali tool documentation	Teach disciplined discovery workflow and note taking instead of broad, noisy scanning.
3	Vulnerability analysis and validation	NIST SP 800-115; CISA Cyber Hygiene guidance	Separate detection from validation and connect findings to remediation priorities.
4	Windows and enterprise attack paths	MITRE ATT&CK Enterprise/Windows; Microsoft Learn Active Directory security modules	Map common Windows and identity attack paths to hardening and monitoring implications.
5	Linux and service exploitation concepts	Linux and Kali documentation; instructor-authored Linux hardening labs	Focus on misconfiguration discovery, service exposure, privilege boundaries, and defensive translation.
6	Web application testing basics	OWASP Web Security Testing Guide; OWASP Juice Shop companion guide	Give students a structured checklist and a legal practice target for common web flaws.

7	Network exploitation concepts	NIST SP 800-115; MITRE ATT&CK; instructor packet-capture or segmentation labs	Connect exposed services, segmentation failures, and pivoting concepts to enterprise defense.
8	Privilege escalation and lateral movement concepts	MITRE ATT&CK; Microsoft identity and Windows administration documentation	Teach the logic of access abuse and movement without reducing the course to exploit collection.
9	Reporting and evidence quality	PTES Reporting; NIST SP 800-115	Standardize screenshots, command logs, timelines, severity narratives, and remediation language.
10	Timed practical: individual assessment	Instructor-authored scenario guide; PTES workflow checklists	Require students to execute a full mini-engagement under time pressure with good documentation.
11	Team scenario: coordination and role clarity	Instructor-authored runbook; role cards; hot-wash template	Practice communication, delegation, and interim briefings in the same operational areas where competitions often fail or succeed.
12	Defensive translation and remediation briefing	CISA guidance; MITRE ATT&CK mitigations; NIST SP 800-115	Require students to convert offensive observations into prioritized corrective action.
13	Optional enrichment modules	OpenSecurityTraining2; picoCTF playlists; faculty-selected challenge sets	Use for stronger students, honors sections, or independent-study extensions without overloading the base

			course.

Recommended implementation note

To control cost, the university could designate NIST SP 800-115, PTES, OWASP WSTG, MITRE ATT&CK, and selected Microsoft Learn modules as no-cost required readings, while any commercial penetration testing text is kept optional. Faculty would then supply the local lab manual, scenario packets, grading rubrics, and reporting templates that tie those references to UNF-specific learning objectives and competition-readiness outcomes.