

PROJECT CHARTER & SYLLABUS

Shimani Alfred Tlokotsi - Cybersecurity Cohort Charter

Date: 7 December 2025

Version: 1.0

SECTION 1: EXECUTIVE OVERVIEW

Project Title: Advanced Penetration Testing Collaborative Learning Cohort

Project Sponsor: Self-Directed Professional Development Project

Project Manager: Shimani Alfred Tlokotsi

Project Duration: 5 Weeks

Total Estimated Hours: 50+ hours per participant

Vision Statement:

To create a transformative learning environment where Bachelor of Technology students can collectively bridge the gap between academic cybersecurity theory and practical, industry-relevant penetration testing skills through structured collaboration, hands-on labs, and professional documentation standards.

Success Criteria:

1. All cohort members successfully configure and maintain isolated penetration testing labs
2. Production of at least 3 professional-grade penetration test reports
3. Development of reusable knowledge management systems
4. 100% participant satisfaction with collaborative learning model
5. Portfolio development suitable for inclusion in professional resumes

SECTION 2: STAKEHOLDER REGISTER

Role	Name	Contact	Responsibility	Engagement Level
Project Manager	Shimani Alfred Tlokotsi	alfredtlokotsi@gmail.com	Overall coordination, scheduling, documentation, facilitation	High (Daily)
Technical Lead	Sibusiso Makhoba	0682551658	Advanced tool support,	High (Weekly)

			methodology validation	
Documentation Lead	Abigail Mbatha	0783256984	Report standardization, template management	Medium-High
Quality Assurance	Yonelani Qinisile	0117629873	Peer review, methodology checking	Medium
Knowledge Manager	Thomas Mahlo	0712440235	FAQ maintenance, resource curation	Medium

SECTION 3: SCOPE & DELIVERABLES

In-Scope:

1. Virtual lab environment setup and configuration
2. Three target systems: Metasploitable 2, Windows 10, Windows Server 2019
3. Full penetration testing lifecycle on each target
4. Collaborative report writing and peer review
5. Knowledge base development and maintenance
6. Weekly progress tracking and status reporting

Out-of-Scope:

1. Production system testing
2. Social engineering attacks
3. Wireless network penetration
4. Mobile application security
5. Physical security assessments

Deliverables Matrix:

Deliverable	Description	Owner	Due Date	Acceptance Criteria
-------------	-------------	-------	----------	---------------------

Lab Environment	Fully configured virtualization setup	All	Week 1	All VMs operational, network communication established
Methodology Document	Standardized testing approach	Shimani Alfred Tlokotsi	Week 2	Covers recon through reporting phases
Target 1 Report	Complete Metasploitable assessment	Team	Week 4	Includes all phases, screenshots, remediation
Target 2 Report	Windows 10 assessment	Team	Week 4	Covers Windows-specific techniques
Consolidated Portfolio	GitHub repository with all artifacts	Shimani Alfred Tlokotsi	Week 5	Organized, documented, professional presentation
Retrospective Analysis	Lessons learned document	All	Week 5	Covers technical and collaborative aspects

SECTION 4: DETAILED SCHEDULE & MILESTONES

Week-by-Week Breakdown:

WEEK 1: FOUNDATION & ORIENTATION

- **Kickoff Meeting:** Agenda includes introductions, goal setting, tool review
- **Lab Requirements:** Minimum 16GB RAM, 200GB storage, virtualization enabled
- **Software Stack:** VirtualBox 7.0+, Kali Linux 2023.3, Windows ISOs, Metasploitable 2
- **Success Check:** All members can ping between VMs by Friday

WEEK 2: METHODOLOGY & RECONNAISSANCE

- **Focus Areas:** OSINT techniques, passive reconnaissance, active scanning methodology
- **Tools:** Nmap, Netdiscover, whois, dig, Shodan (free account)
- **Collaborative Task:** Each member researches different reconnaissance tools

- **Deliverable:** Reconnaissance checklist and tool comparison matrix

WEEK 3: SCANNING & ENUMERATION

- **Technical Depth:** Nmap scripting engine, service fingerprinting, vulnerability scanning
- **Tools:** Nmap advanced scripts, Nikto, Enum4linux, SNMPwalk
- **Lab Exercise:** Full port scan with service detection on all targets
- **Deliverable:** Service enumeration report for each target system

WEEK 4: VULNERABILITY ANALYSIS & EXPLOITATION

- **Methodology:** CVE research, exploit selection, safe testing procedures
- **Tools:** Metasploit Framework, Searchsploit, Exploit-DB
- **Ethical Considerations:** Discussion of responsible disclosure
- **Deliverable:** Vulnerability assessment matrix with risk ratings

WEEK 4: POST-EXPLOITATION & REPORTING

- **Techniques:** Privilege escalation, persistence, lateral movement
- **Tools:** Meterpreter, PowerSploit, Mimikatz (in lab only)
- **Documentation:** Report structure, executive summary writing
- **Deliverable:** First complete penetration test report

WEEK 5: ADVANCED TOPICS & TEAM COLLABORATION

- **Focus:** Windows-specific attacks, AV evasion basics, clearing tracks
- **Collaboration:** Cross-review of reports, methodology refinement
- **Team Challenge:** Capture-the-flag style exercise
- **Deliverable:** Second report and peer review feedback

WEEK 5: CONSOLIDATION & KNOWLEDGE TRANSFER

- **Portfolio Development:** GitHub organization, README creation
- **Retrospective:** What worked, what didn't, lessons learned
- **Knowledge Transfer:** Creating guide for next cohort
- **Final Deliverable:** Complete project portfolio and final presentation

SECTION 5: COMMUNICATION PLAN

Regular Meetings:

- **Weekly Sync:** Wednesdays 7:00 PM via Discord
- **Duration:** 60-90 minutes
- **Format:** Roundtable updates, technical deep dive, Q&A
- **Recording:** Sessions recorded and stored in shared drive

Communication Channels:

1. **Primary:** Discord Server with channels: general, #technical-help, #report-review, #resources
2. **Secondary:** Email for formal notifications
3. **Documentation:** Google Drive for collaborative editing
4. **Code/Artifacts:** GitHub repository

Reporting Structure:

- **Daily:** Informal check-ins via Discord
- **Weekly:** Status report due each Monday at 9:00 AM
- **Milestone:** Formal review at end of Weeks 2, 4, and 5

SECTION 6: RISK REGISTER

Risk ID	Risk Description	Probability	Impact	Mitigation Strategy	Owner
R01	Technical difficulties with lab setup	High	Medium	Create detailed setup guide, offering one-on-one support sessions	Shimani Alfred Tlokotsi
R02	Participant drop-off	Medium	High	Regular check-ins, engaging content, peer accountability	Shimani Alfred Tlokotsi

R03	Scope creep	Medium	Medium	Clear charter, weekly scope review, change control	Shimani Alfred Tlokotsi
R04	Knowledge gaps slowing progress	High	Medium	Pre- assessment, just-in-time training, buddy system	Technical Lead
R05	Time constraints	High	High	Realistic scheduling, flexible meeting options, prioritized tasks	