

IT Capstone Topic Approval Form

The purpose of this document is to help you clearly explain your capstone topic, project scope, and timeline and to ensure that they align with your degree emphasis. Without clearly addressing each of these areas, you will not have a complete and realistic overview of your project, and your course instructor cannot accurately assess whether your project will be doable for the purposes of these courses.

Of course, if this a project that you have already completed at work or elsewhere, this should be easy to fill in! Most students use a project that they have already completed in the past year or two. In that case, you will write the proposals (Tasks 1 and 2) as if the project has not been done yet, and Task 3 as the complete post-implementation report.

Complete this form and send it (via UGCapstoneIT@WGU.edu) to your course instructor for approval. Once approved, you will receive a signed document in PDF format that you can upload as part of Task 1.

DEGREE EMPHASIS:

Cybersecurity and Information Assurance

ANALYSIS:

Project Topic –

Penetration Testing in the Army Cyber School Training Network

Problem Statement or Project Purpose –

Demonstrate proficiency in penetration testing including network reconnaissance, lateral movement, privilege escalation, and establishing persistence

DESIGN and DEVELOPMENT:

Project Scope

a. Project Goal(s) and Supporting Objectives –

Successfully exploit hosts on the network

b. Project Outcomes and Deliverables –

Map the network, recover flags, document all actions taken on the network, and provide remediation suggestions to remove vulnerabilities


c. Projected Project End Date - 24 Oct 2022

IMPLEMENTATION and EVALUATION:

Describe how you will approach the execution of your project –

Sniff traffic using Wireshark and tcpdump, as necessary. Perform host discovery using nmap, exploit vulnerable services or obtain credentials to gain access to the network. Escalate privileges either using tools such as Metasploit or system misconfigurations such as SUID binaries. Begin lateral movement while establishing persistence along the way using reverse shells, ssh tunneling, and/or cronjobs. Finally, I will report all steps taken, vulnerabilities found, and remediation options to mitigate them.

☒ This project does not involve human subjects research and is exempt from WGU IRB review.



James Allen, PhD

COURSE INSTRUCTOR SIGNATURE:

COURSE INSTRUCTOR APPROVAL DATE: Monday, October 17, 20