THE
ASCENDANCY
GROUP

OFFENSIVE CYBER OPERATIONS- INTRODUCTION TO PENETRATION TESTING / RED TEAMING

COURSE OVERVIEW

This 10-day instructor led course is designed to prepare personnel for operations as a penetration tester or Red Team member. Prior to attending, students must have at least a familiarity with Linux Operating Systems. The course begins with an introduction to the Penetration Testing Methodology and follows NIST 800-115 guidelines and requirements. Students do not need any previous experience with penetration testing. Students will leave the course with a thorough understanding of how to plan a penetration test, conduct information gathering, conduct exploitation techniques for initial access, conduct post-exploitation techniques, and finally how to conclusively write a qualitative and quantitative report of the test they performed and state the potential impact.

COURSE OBJECTIVES

- Legal brief and disclaimers, intro to the lab environment
- Penetration testing model, theory
- DOD or financial industry reference documentation (as required)
- Log and accountability maintenance
- Open source research and analysis
- Passive and active scanning and analysis
- Target system / network enumeration and analysis
- Social engineering and remote access
- Denial of service operations - Application and network layers
- Initial access - The first compromise
- So you got a shell…. now what?
- Situational awareness and follow on enumeration
- Gaining persistence
- Escalating privileges
- Password harvesting
- Data harvesting
- Generating keyloggers and spyware
- Pivoting through the network
- Cleaning up
- Team management
- Final team exercise