**ULM Security Boot Camp -2018**

**Hands Information Security Assurance Testing**

**Objective:**

**The primary objective is to give the attendee hands on experience in performing a “typical” IT security and compliance review. The course will introduce a methodology and set of open source tools that will enable the attendee to perform a security audit/compliance review in a teaming environment. What is different form the previous years is the introduction of Artificial Intelligence into the security equation.**

**Area’s that will be covered include:**

* + 1. **Introduction to Information Security and Engagement Planning (Allen)** 
       1. **Your First Job in Security**
          1. **IT Audit**
          2. **Security**
          3. **Risk**
       2. **Scoping**
       3. **Engagement Letters**
       4. **Rules of Engagement**
    2. **Risk Assessments (Ross)**
       1. **Types**
       2. **Methodology**
       3. **Execution and Case Study**
    3. **Social Engineering** 
       1. **Using the Internet to Obtain Information**
       2. **Phishing Techniques**
    4. **Social Engineering (Lab) –(Team)**
       1. **Practical experience in creating and executing phishing attack.**
       2. **Execution of the Attack**
       3. **Execution of Power Shell Malware**
    5. **New Technologies (Ross)**
       1. **Networking**
       2. **Internet of Things**
       3. **Cloud Computing**
       4. **The Dark Web**
    6. **Application Security – Allen Lum**
       1. **Application security Issues**
       2. **SQL Inject –Cross Site Scripting Etc.**
       3. **OWASP**
       4. **Hack Me Lab - Ross)**
    7. **Application of Artificial Intelligence to AI**
       1. **Introduction to AI**
       2. **AI Models**
       3. **Regression**
       4. **Neural Networks**
    8. **AI Labs**
       1. **Prediction**
       2. **Regression**
       3. **Neural networks**
    9. **Open Source Security and Network Assessment tools – (Allen)**
       1. **Networking Scanner** 
          1. **Nessus**
          2. **NMap**
          3. **Web / Command Line – Getting Information from The net**
          4. **Capture the Flag**

**Security Policies and Procedures to Mediate Risk - Ross**

* + - 1. **Compliance**
      2. **Testing Compliance**
      3. **Internal Security server Lock Downs**
    1. **Reporting - Allen**
       1. **Target Audience**
       2. **Reporting Examples**

**This course is not an – Attack and Penetration course. However many of the tools used in an Attack and Pen test will be demonstrated in this course.**

**Format: The class will format will be divided into 9 sections. Each section will entail an about 1 hour of lecture and 2 hours of hands on lab.**

**Teaming: We will be taking a teaming approach to the labs. In the real world the loner will not succeed. There are too many specialties within information security**