Alexander Cannell

CSIA 6210

**Week 3: The business of pen testing**

**My Thoughts about the 7 Stages of Penetration Testing:**

Starting this course I had the question in mind even though I didn't know what open source intelligence gathering was called at the time; “how do we perform an Open Source Intelligence Gathering?” I’m glad we are going to address this later on in the course. In class, we have done a lot with testing tools and performing private isolated network tests of those tools. I’m excited to learn OSINT.

The separation of mapping and enumeration was kinda weird to me at first. I always assumed that the information gathering stage included mapping enumeration stages of the Pent Testing Stages. I always thought of pen testing in three stages; Information Gathering, Exploitation, and Reporting/conclusion with the need sub-stages. But that would make sense to separate all three. In our undergrad ethical hacking course we would do that process of mapping then enumeration then moves on the exploitation or the testing of some of our tools.

When I was going through the 7 Stages page I was wondering, “How do we account for people whose main goal is to do harm(do damage) in the system?” I assume that if you are able to escalate and get to a point where you can exfiltrate, the situation is assumed that the attacker can do harm. Last semester I took the Info Security Communications class where the Professor brought up the same point, “it's one of the reasons that pen testers need to be more than good hackers but also good communicators.” He told us that as security professionals we need to be great storytellers. We need to have the ability to explain what happened and how the issue happened to non-tech-savvy people. I work for a SOC(Security Operations Center) and the majority of what I do is write emails/reports explaining what happened so that people can understand. Sometimes writing in a general way is hard to do, when writing in a technical way would be a lot easier and less time-consuming.

**My thoughts about Engaging for Penetration Testing:**

The major thought I had while reading about the business aspects of consulting was wow there are a lot of countermeasures for not being sued after a penetration test. In past classes, we discussed a lot about contracts for White Hats and Pen Testers. We addressed the need for full disclosure and privacy. I assumed that a NonDisclosure Agreement would have to be in play for a pen tester. This is kinda like a first date, let them know your expectations, they let you know their expectations, you have a lawyer on hand for any legal issues, both agree to the rules of engagement, and sign the contracts… If you were asking is this how he really dates, I will answer no. But maybe I should, especially the setting expectations would probably save me a lot of headaches. I found the setting expectations with regards to consulting quite interesting because I can imagine not every Pen Test goes according to plan. Addressing/calming concerns, and warning the customer before hand could really help the company be prepared. I work for Ancestry.com and we have an in-house penetration tester. I was able to talk to him about the differences between consulting and in-house. he said he has to go through these steps. Except he doesn't have to sign an NDA or MSA, just a SOW. He also noted that he is in constant contact with our legal team.

Honestly, I thought I had a good understanding about the business aspect of Pentesting from previous classes. But I can see now it takes a lot more work than signing some contracts and hacking. I learned the importance of setting expectations, and communication between parties.