**CYBR430 Penetration Testing and Incident Response**
**Term Project Scenario**

You have been hired by Happy Accident Labs to conduct a penetration test against their organizational network. The below summary provides a limited background on Happy Accident Labs, and gives you enough information to begin your work.

---

# Happy Accident Labs

**"Smarticle Particles for Better Living"**

Hi, welcome to Happy Accident Labs. My name is Bill Winnicott and I'm the CIO here. We are a new start-up in Omaha, Nebraska focused on developing miniature (I mean really small) Internet of Things (IoT) devices which will serve as personal assistants, they will do everything from search information on the web, to manage your schedule, to order groceries or take-out when your fridge is empty. We call them smarticle particles. We are really excited and are just about to get our second round of venture capital funding, we can't afford any missteps right now. And, that's why we hired you.

Our team is 100% focused on getting to our next prototype so our IT system has been pretty much flung together. It works, and up to this point we have seen little need to change what we are doing. One of our potential investors is very concerned that our intellectual property (IP) may be stolen and a competitor could beat us to market. We don't think that is a possibility, but the investor has required that we have a penetration test done prior to her putting her money on the line. We've been told we need a black-box test, hope you know what that means because none of us do. Our chief scientist, who is a physicist, thought it may have something to do with a cat, but we doubt that is the case.

So, what we need is a black-box penetration test of our network, we want to know if there are any vulnerabilities we must address to keep our IP safe and secure. We would also like your recommendations of what we should do to address the vulnerabilities you find. When you are complete we need a penetration test report with your recommendations and risk assessment.

The scope of the test is our entire organization internal network. We use private IP space in the range 10.19.99.1 - 10.19.99.99. You are not authorized to test outside of that range of IP addresses. You have permission to conduct the test on all company owned assets, to include scanning and client access, **but not on the networks of any of our clients or suppliers.** This means any services we outsource, such as our public website, can be viewed but you may not attempt to hack it. Our teams can't stop work while you do the test so although you can use any access you gain you are not allowed to impact the operation of any system. We just did a phishing test with another vendor and it pointed out lots of items we need to work on. We haven't completed those actions yet so no need to retest that. This means you are not allowed to do any social engineering for this test. The building we occupy doesn't allow physical pentesting, we understand the last group that tried without authorization could be out of prison in 5 years on good behavior.

If you have any questions let me know. Good hunting.