The topic for this week is to introduce and discuss the hacking mindset and psychology. The resources for this week are:

* 2013 Article by Joshua Hickernell: [Knowing the Opponent: How understanding hackers can enable more comprehensive computer securityPreview the documentView in a new window](https://suu.instructure.com/courses/355040/files/51850629/download?wrap=1)
* Bank Info Security - Interview with David Pollino: [Understanding the Hacker Mindset (Links to an external site.)](http://www.bankinfosecurity.com/interviews/pollino-i-2589)
* Cybereason Blog: [6 Reasons Why Hackers are ahead of the Game and Tips to close the gap (Links to an external site.)](http://www.cybereason.com/6-reasons-why-hackers-are-ahead-of-the-game-and-tips-to-close-the-gap/)

1. Read/Listen to the above sources
2. For your initial post address the following:
   1. Summarize what your thoughts are in regards to the "hacker mindset".
   2. Why do hackers seem to always be one step ahead of the good guys?

**Grading:**

* Initial post = 25 points
* Comments on other student posts (2 posts) = 10 points
* Post of other resource (can be articles addressing controls or events relating to ethical hackers) = 5 points

1. Summarize what your thoughts are in regards to the "hacker mindset".

The article, “knowing the Opponent: How understanding hackers can enable more comprehensive computer security” by Joshua Hickernell was my favorite out of the three articles we read. He splits up his paper into two sections one, the psychology of the hacker and two the stages every hacker goes through so the physical. My thought regarding the psychology behind hacking is he is only looking at hackers one way. The way being all hackers are motivated by one thing and that is profit. “Today, hackers are 2 motivated by a desire to gain money from their exploits.” I think that Josh is missing alot of different motivations, I think forsure hackers are profit is one of them. Some I can think of off the top of my head is self fulfillment, understanding how things work, protection of companies, bragging rights, to humble companies, testing of skill, gain of power, boredom, recognition, and yes profit. I love how he brings up the different skills a hacker need to have other than an understanding of how computer systems work and programming skills. The other skill he mentioned was people skills. I totally agree, the weakest element will always be the human element. Adrian Lamo a grey hat hacker explains his mindset in this video, “hackers wanted’. He earlier explains that how he got into hacking is a curiosity of finding out how things work. <https://youtu.be/vSBzKEdSPMY?t=1h7m16s> A hacker has to have the skills of a grifter now a days too, social engineering plays a vital role in the scanning and vulnerability identification stage of his “stages of attack.” He has four stages of an attack, first Reconnaissance; second scanning and vulnerability identification; third exploitation; fourth maintaining access and covering tracks. Reconnaissance gain as much information you can about a target. He explains there are two types of reconnaissance passive and active. Scanning is the process of using different processes to find vulnerabilities in a system. Exploitation is after finding vulnerabilities they attempt to gain access. I believe this part of his paper was really well written.

Here is a research paper similar to joshua’s: <http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf> . In it has a really interesting self assessment by hackers. where it goes into more depth on psychology behind hacking. Interesting read.

The article Understanding The Hacker Mindset, by Tracy Kitten interviewed David Pollino a Fraud Prevention Officer for the the Bank Of The West. What I found interesting was he said in his interview with ISMG is that security officials need to share what they have learned with others such as peers, law enforcement, regulators, and other industries. If we are to stay ahead of an enemy we need to have some support and information from others trying to defend against the same attacks. Hackers have a hive of information, so should we. "It is important for us to have a strong external and internal intelligence practice. Once we learn things, how do we share that back to the greater community? That's a key component of intelligence.", said David. Bank of the West has set up a forum for other SOC Teams to post, and get information on current attacks methodologies.

Reading the “Six Reasons Why Hackers Are Ahead Of The Game And Tips To Close The Gap” I thought gap number 6 was very interesting, it says that SOC Teams are overwhelmed with the number of incidents large amount of alerts and false alarms, and hackers use these distractions to distract from the real attack. I think they call it a diversion. Kindof like a DDoS attack but instead of overwhelming number of ping packets they are sending up false alarms. I love the solution to overcoming large amounts of incidences. make a timeline of the events; Find the root cause; take countermeasures; have good communication. Hacking is really a type of warfare, the strategies just listed in this article are good strategies to use on a battlefield. Take six, overwhelm your enemy with a large amount of minor attacks to disguise the major attack in progress.

How hacking has been incorpiated into modern warfare: <http://usnews.nbcnews.com/_news/2013/02/19/17019005-successful-hacker-attack-could-cripple-us-infrastructure-experts-say?lite> an example in 2013 of the possibilities of the US being crippled by an attack. How China has already tried. (which I dont see how that isn’t an act of war)

After reading these articles I have determined that the mindset of hackers have to be continuously evolving, Knowing many different skills, have a curiosity, and be determined/dedicated. Honestly I think the hacker mind is one of the most brilliant mindset in the world. The way they can take a problem apart and look at how the thing works, where the holes are, and find a way in….scary but brilliant. So we as cyber security experts need to be smarter then the next guy.

2. Why do hackers seem to always be one step ahead of the good guys?

In the article we read, “Six Reasons Why Hackers Are Ahead Of The Game And Tips To Close The Gap” it states that, “Hackers are determined to penetrate a network and have a 100% success rate. There are hundreds of ways to penetrate a company’s perimeter and an ambitious hacker will surely find one.” I believe that is the main reason why hackers are one step ahead of the SOC Teams. I think that every “gap” stated by yonatan striem-amit is are good reason why the “good guys” are behind. but the underlying issue is there are always going to be a way in. The easier something is to access the less secure it becomes. In order for work to get done you have to have some access to the system.The reason they are ahead is because they are the ones performing the attacking, kindof like battleship a hit and miss system. but it is the goal of the SOC to take it from a battleship game to a chess game where you are playing offensively and defensively. A good chess player plays both offensively and defensively at the same time, also seeing several moves ahead. The bad chess players are the ones who only react to the other players moves. As a SOC Team and as a good board game player you have to have a good plan for when security incidents happen, sure up your defenses, and to be uptodate. David Pollino stated in his interview, “You not only need to know your attacker, but also what their tactics are.” Such a true statement.