Guest Lecture Makeup – Lecture 4

This guest lecture was held by cyber security workers at Avanza, a Swedish brokerage firm, who divided the lecture in two parts. The first part was held by Camilla, who is head of IT Security and Cyber at Avanza, and the second part was by Levi, who has been a security analyst at Avanza for the past two years.

The first talk by Camilla started with the topic “thinking like a boss”. She spoke about Avanza, giving some ground statistics about it, and spoke about cyber security’s role at a place like Avanza. She spoke about having to create her own cyber security team and the struggles with that. To create an expert team, she needed to get what she coined as a “red teamer” and a “blue teamer”. A red teamer is an offensive expert. This means someone who is very knowledgeable on how to attack systems. They can be very useful at visualizing a problem and helping the team understand it. The blue teamer deals with the defensive aspects of the job. They focus on how to protect against vulnerabilities that the red teamer has found. They are equally important for a good cyber security team. She then pivoted to talking about the mindset you need to have in cyber security. This means analyzing which threats they have to protect against, and there were four threats to beware of: the script kiddie, the evil hacker, the insider, and the rival. While the script kiddie and evil hacker are worth noting, they are generally not so dangerous or prevalent given that the script kiddie will only use commonly known programs and should be relatively easy to stop. The evil hacker, while potentially dangerous, is significantly less common, making it a smaller worry. Insiders and rivals are what one really has to watch out for, as they have the potential to be very good at what they do, and they have more of a motivation to attack the company. Camilla also mentioned the kinds of jobs you could get as an ethical hacker, namely by either working for a company in the cyber security department, or by participating in

bug bounty programs and other opportunities that let you legally find and report vulnerabilities to companies. These are programs that are mutually beneficial to companies and hackers involved. The main purpose of Camilla's talk was to not only give the audience an idea of what it's like to work as a cyber security specialist at companies, but also to give an idea about the mindset that is required when doing such a job. Camilla then took in questions from the audience and passed the floor on to Levi.

The second talk by Levi, a security anaylist at Avanza for the last two years and was more of a technical talk than Camilla's. Levi is a blue teamer at Avanza and therefore had a lot to say about defensive hacking. Levi started by talking about an attack chain. This attack chain was somewhat similar to the different "stages" of hacking that we also learned about during our course, in that it included most of the same stages (execution, persistence, privilege escalation, data exfiltration, etc.), but also had significantly more stages (lateral movement, defense evasion, etc.). He spoke about how when a vulnerability of these types is found, they report this, and then the blue team must classify it by deciding how far the hacker came, where they are right now, and how bad the vulnerability actually is. This is all handled by the SOC (Security Operations Center), which includes several set processes and solutions in order to most efficiently identify these vulnerabilities as well as classify them. He talks about these methods by mentioning SOC fundamentals. Levi then moves on to talk about an extremely important framework: OSINT. This stands for open source intelligence, and is extremely useful for threat intel. In layman's terms, OSINT refers to being up to date with, as well as personally contributing to the cyber security community. OSINT is extremely important in our modern day world where new vulnerabilities are being found every single day. Because of this, a company that doesn't stay up to date will not be able to adequately protect themselves against new vulnerabilities. Going more

in depth, Levi now talks about detections and anomalies. Detections are events of interest to a security analyst. An example is a command on the PowerShell that downloads mimikatz onto the system. Something that, while not a vulnerability per se, is undesirable for cyber security purposes. Anomalies are defined as unlikely or odd events. An example of this is a user who has submitted an abnormal amount of wrong passwords. This is notable because hackers will almost always perform anomalies (especially if they are not so experienced). By searching for anomalies, you might find someone trying to break into a system. Levi then gives us a practical technical scenario. He describes the event as finding an event log that says that a user has failed to log in to an account. While this is not usually abnormal, what is abnormal about this scenario is that the user tried to login as administrator (or some other default account). Then, it is noted that this login came from an unusual subnet (not the office subnet that people usually log in from every day), and we also notice that the device accessing is a non-compliant device. Finally, the MAC address is from a Raspberry Pi. Eventually, they found a Rasperry Pi connected to a wall in the company, which was actually planted by the red team! All this information was found because of one single failed login. He concludes by mentioning how important it is to be stealthy when hacking. Levi then gives a few more technical examples and takes in questions from the audience.