Guest Lecture Makeup – Lecture 3

This guest lecture was held by a member of the Swedish Security Service. He divided this lecture up into two separate sections. The first section was dedicated to being an overview of what the Swedish Security Service actually does. The second part talks about ethical hacking at the Swedish Security Service. Notably, penetration testing and extracting data from devices.

The first part of the talk begins by talking about the mission of the Swedish Security Service. Their mission is to prevent, detect, and investigate any kind of threats to national security of all forms in Sweden. He mentions how, in Sweden, two institutions have police authority: the National Police Agency, and the Swedish Security Service. The type of crime is what differs which institution deals with it. The Swedish Security Service deals with national security crimes, so things like terrorism and espionage, whereas the National Police Agency deals with all other types of crimes, such as drug-related or gang violence crimes. Security at the Swedish Security Service consists of three important components (or types of security): physical security, personnel security, and information security. All of them are equally important. Physical security deals with protecting areas. So thickness of doors, types of locks, etc. all matter in this subject. Personnel security deals with protecting members, and information security, of course, deals with protecting data. He mentions how because most of the data the Security Service works with is not available to the general public, they must have a lot of oversight from other separate institutions to ensure that everything they are doing is legal and that they are not overstepping boundaries. This is important for any democracy. He then moves on to talking about different methods by which Sweden (and by extension any country) might be attacked. He first talks about espionage. Espionage is useful for countries that want data on Sweden for personal purposes. They might attempt to obtain industry secrets or other important information

(military installations and capabilities, etc.) that will benefit the foreign power. Because of this, it is extremely important that this classified information stays classified, and the Security Service must put a high priority in defending against these kinds of attacks. Another danger for Sweden is terrorism. For self-explanatory reasons, terrorism is an event that must be prevented before happening. Because of this, counterterrorism is also of utmost importance for Swedish national security, so attacks may be predicted and stopped before they happen. Two examples of terrorism that were given was a suicide bombing in 2010 in Stockholm, as well as an arson on Lars Vilks's house due to a controversial cartoon drawing they made of the prophet Muhammad. The NCT raised Sweden's threat level from "low" to "increased". ISIS is also mentioned as a danger. With the rise of social media, this is something terrorist groups often use to communicate with each other. This means this is a good attack point for the Security Service to try and find these terrorist groups and intercept information about future terrorist attacks. It is mentioned how there are often four stages to a terrorist attack: talk and ideas, reconnaissance (of the terrorism target), obtain money/weapons/equipment, set plan into action. There is a dilemma which is that, even though of course we want to stop it as early as possible, the earlier you stop the terrorist attack, the less evidence you have, and the less people you might actually convict. Many attacks also skip the third stage (such as, for example, the Drottninggatan truck attack).

The talk then segues into the second part, which talks about the types of ethical hacking that are employed at the Swedish Security Service. Firstly, he mentions the importance of penetration testing. Penetration tests are used to ensure that IT networks can resist intentional attacks and are extremely useful for defensive hacking. This is also somewhat required due to the Protective Security Act which was passed into Swedish legislation in 2018. This act applies to anyone conducting activities regarding national security in Sweden and contains regulations

about the types of security and precautions that are necessary when conducting said activities. The Swedish Security Service has both a duty to adhere to these regulations, but also has an oversight role of ensuring that anyone who this law applies to might also be adhering to the regulations. We then go over several technical penetration testing methods, and we classify them into three types of tests: black box, white box, and grey box testing. In black box testing, the attacker and defender work completely independent of one another. In white box testing, the attacker and defender are fully aware of each others' work. In grey box testing, it is a mix between the above two classes. White box tests are usually done at the Security Service as they seem to produce the best results and learning experienced for everyone involved. After talking a bit about what kind of assignments and activities you do as an ethical hacker for the Security Service, we move on to talking about data extraction. This involves finding data in a seized device of, for example, a terrorist. It also involves extracting data without physical access to a device. This will ideally also be covert and the victim will not know about it. This is called secret data extraction, and it dates back to the 1990s. This type of data extraction must, of course, be done through some kind of network, and must intercept signals in said network. If there is no data being sent between two devices, there is no way to intercept that data without physical access to the device. In recent years, several countries have implemented laws that allow for secret data extraction from people who are suspected of being involved in certain serious crimes. This kind of secret data extraction requires a court order and must specify the period of time during which data will be extracted, the targeted information system, and what kind of data will be collected. Urgent cases may have exceptions that allow for data extraction to happen faster. Data extraction may never be used by journalists, lawyers, doctors, or any other profession for

means other than those of national security (which is decided by a court order as mentioned above).

The lecture is then concluded by posing the big picture challenge of cyber security for most democratic countries: creating technologies, services and procedures that find the sweet spot between allowing enough data interception for national security, without overreaching so that the government has too much data and power over its people, all the while not introducing high levels of regulation that will impede new techniques from being found.