Question 1 (10 points)

In the discussion of **attacker profiling**, we have stated that an adversary would aim to maximize the gain that can be reaped from an attack, and likely **forego** an intrusion attempt **if** the return on investment (ROI) is **negative**. ROIs do not have to be strictly **monetary**, an adversary may also pursue **non-financial motives** and thus compute value differently.

Exemplify this issue by **discussing different types of objectives and gains some adversaries are after**. Describe **why an attack could still be worthwhile for these actors given a negative monetary ROI**.

Attacker Profiling is the concept of separating the infrastructure properties from unauthorized access, disclosure, modification and interruption by using strategic decisions of security like encryption.

Gains and objectives of adversaries: The discovers who are software engineers find a vulnerability and as many organizations do not offer much incentive for discloser turn to underground forums and market for Monetary GAIN. To a script kiddie availability of botnets helps them to execute DDOS attacks for a bargain price and the gain for him is less investment in making spam mails as botnets take care of them. The medium skilled cybercriminal who has objective who is well-funded can gain by buying the third-party tools and services for a crime operation even if he has less skills for launching an attack- this gives him the gain of not disclosing his skillset level to other criminals. Inside attackers with the objective of revenge to simple monetary gain. The cyber terrorists objective is to damage the infrastructure making it permanently inoperable and monetary damage to dependent on the infrastructure.

Worthwhile even if attack have negative monetary ROI: This is because of political and ideological reasons as it gives the well-funded hacktivist the satisfaction of having made political statement even at considerable expenses, similarly a nation-state actor does not have to worry about creating profit in its business unit at the end of the year. Hacktivists and vandals want to obtain publicity as a gain and the objective is to promote social or political agenda. The nation state actors / state sponsored attackers have the motive ranging from reconnaissance and monitoring government of another country, theft of intellectual property and install “kill switch” to be used later.

Question 2 (10 points)

Preparing and testing the **effectiveness** of a network security plan requires the **defender** to also have offensive capabilities: one needs to understand **how and using which tools an adversary** is likely to attack to improve the lines of defense and to train for an emergency. Such **testing** may take many forms, such as commercial penetration testers, but also a **bug bounty program** where an organization pays freelance hackers on the Internet money for every **vulnerability** they find and disclose to the organization.

Research the **legal context** of network security and vulnerability testing in your jurisdiction, **what is allowed and what not**?

Under **which circumstances may you scan and probe** your own and someone else's network and computing systems?

Allowed and Not Allowed in Network security and vulnerability in my jurisdiction and circumstances where I can scan and probe are as follows: 1. Protect the privacy of personal data (online privacy), 2. Processing of person's religion is not allowed, 3. Prohibition or processing of personal data without consent, 4. Protection of personal data of the telecommunication networks subscribers 5. Transfer of personal data of a person to a third country is not allowed but it can be done if it attached with more rules of how the personal data can be protected and on the duration of this planned process of transferring personal data and on the legal provisions of the third country concerned, 6. Building of personal profiles using the data from cookies is not allowed and is a violation of privacy laws and needs unambiguous consent of the user for using the information that the cookies collect and needs to provide the purpose of collection and storage of such personal data by the cookies, 7. Authorities in Netherland allow data retention for the investigation and prosecution of serious offences 8. Mass monitoring of phone calls, internet, email traffic, text messages and website visits are allowed, and the Dutch government can hand this to international agencies for analysis, 9. Profiling and behavioral analysis is allowed 10. Hacking of third party application is allowed, 10. A third party hacking tool can scan networks of interest is allowed, 11. Cryptographic keys of customers can be handed over to agencies conducting analysis. 12. The vulnerabilities are Territorial integrity to function as an independent state , Physical security of people, Economic security, Ecological Security, Social and political stability and to safeguard from these dutch government does periodic security audit and system penetration tests, information physically located in Netherlands.

Question 3 (10 points)

Derive a **comprehensive attack tree** for the bridge scenario depicted in the figure from the first lecture (slides are on brightspace). Discuss **why** it is important to **also include vectors** which are **already** mitigated or out of scope **in terms of** risk treatment plan in such an attack tree.

The attack tree diagram can be found in the following link:

https://docs.google.com/presentation/d/e/2PACX-1vQqqnSezImH_A8yoBmPRwF43_rWHkUdyMNWtwiV4_Llhjnhq0AV1laBDnIcL_MrbjYkpYjOwtwpOSCx/pub?start=true&loop=false&delayms=3000

To arrive at a comprehensive risk analysis it is good practice to include all identified possible scenarios, even if considered irrelevant for the organisation's defense plan. It is important to include such vectors as it is possible in a later revision of the plan to differentiate whether a particular scenario was 1. Identified as threat, 2. Identified but discarded out of scope, 3.consideredimpossible to occur. This prevents accidents that happen due to incomplete assessments and incorrect conclusions drawn upon them. A limited budget can be allocated to maximize the mitigation of expected risks. Implementing a control resolves the vulnerability. Vulnerability describes the specific weakness that may be exploited while threat refers to the event and action of exploiting it. A good

quantification risk and treatment helps allocate resources in those spots in terms of risk and impact and generate more benefit.

Question 4 (10 points)

Cloppert et al. argue that when following a "**kill chain''** network security **model**, the **defender** actually has a **competitive edge** over possible adversaries. Summarize and explain **two major aspects** of this competitive edge.

“Kill Chain” or intelligence-driven network model.

1. Two major aspects of competitive edge of the defender: Realising and exploiting the fact that an attack is comprised of series of individual activities provides a competitive advantage. The first aspect is that analysis and synthesis of mitigated attacks increases the odds of the defender to detect and prevent related incursions in the future. And it allows the organization to improve intelligence about the threats it faces, as individual attempts that share one or more aspects of the chain (same vulnerability, same Command and Control protocol) may be attributed to same actor, resources like infrastructure or software that is common. The reuse of components and knowledge that the attaker uses will give the defender an competitive advantage.

The second aspect is that all the elements of the chain add up to be watched out. As the defender stops threat at each item, which increases the chances of future detection of outcomes along the other chain elements easy. Unless the attacker invests and redesigns each component after each detected attempt, it will increase the cost of operation for the attacker and decrease his return of investment and deter attacker from future attack activities on the organization.

Extending the detection towards all phases of attack progression and not only the exploitation of virus scanners and intrusion detect system will greatly increase the odds for the defensive side. If the defending party detects the attacker before he is successful in every step, then defender will have sudden advantage of interrupting the chain at any single element that will avert the damage and let the attacker fail. When the probability of probability of defense gets better in an increasing fashion it is a competitive edge. Only if there is sufficiently high detection probability the defender can gain competitive edge.