RE-EXAMINATION IN CYBER SECURITY

August 10th, 2020

The re-exam consists of two (2) questions, which are in total worth thirty (30) points. Partial credits of 0.5 points will be provided. The maximum number of points that may be accomplished is thirty (30) points. In order to pass you are expected to attain at least eighteen (18) points. Only answers in English will be accepted. If you attach a file or a drawing write eligible. **Unreadable answers will be failed.**

Note! You must clearly specify any presumptions made.

Best wishes for a successful and profitable work. Lycka till!

Scenario

Crisis Management Ministry of Caledonia has received information concerning a breach of political parties' servers. The reports state that the hackers have been able to seize sensitive information from the servers and there are suspicions that insiders might have been involved in facilitating the operation. Several unexplained disturbances have also affected electricity supply, train and air traffic management, and has created confusion and uncertainty. An announcement on the Darknet calls for individuals hired at key companies and/or government authorities who are willing to sell information that may yield political consequences. Financial institutions have been the subject of denial of service attacks, which has led to problems with banks' payment applications. In addition, based on these and other events, it is discussed loudly in the media about the authorities and other actors' inability to secure sensitive information and protect privacy. With the ongoing Caledonian elections, there are indications that foreign powers have an interest in trying to influence the election process. The cyber incidents are affecting the Caledonian finance institutions, health sector as well as political parties. The nature of the incidents, as well as nation-state dependencies and industry vulnerabilities means that the task force must act swiftly to allay concerns from the private sector and international partners.

Q1.

Apply the incident response process and resolve the situation in Caledonia. Consider all aspects of the presented scenario. Your solution should be realistic.

Q2.

Model two attacks from the given scenario and explain (step-by-step) how an adversary can reach its ultimate goal. For each step, define one or two countermeasures (security controls) that prevent the attacker's from reaching the ultimate goal.