Possible Solution

- Describe a maximum of 3 different actions (which are unintended by MEGACORP) an attacker could perform by exploiting the critical vulnerability on the Exchange Server (Mars)?
  - An attacker can read the contents of all mailboxes
  - An attacker can write files to the file system of the Exchange Server (WebShell)
  - An attacker can execute commands as LocalSystem and Exchange Trusted Subsystem and thus e.g., changing Exchange configuration, exporting mailbox etc.
  - An attacker can use the Exchange Server as a jump host for further attacks against the complete network
- Describe a maximum of 3 different actions (which are unintended by MEGACORP) an attacker could perform by exploiting the critical vulnerability on the Domain Controller (Pluto)?
  - An attacker can change / remove a service account on the Domain Controller (and thus gaining control over the DC)
  - An attacker can harvest credentials (and then execute attacks such as golden ticket, pass-the-hash or silver ticket attack)
  - An attacker can download malware (if internet is routed in the network see question 3) and distribute it laterally
- Under what technical circumstances the critical vulnerability on the Domain Controller (Pluto) is most problematic?
  - Routed internet in server network
  - Accepted inbound-connections from untrusted zones (on DC)
  - Misconfigured Firewall / Router
  - …
- List a maximum of 2 different immediate actions be taken in the given scenario.
  - Patching the vulnerable systems (Mars & Pluto)
  - Checking whether the vulnerabilities already have been exploited and changes has been made to systems
  - Disconnect the DC immediately from internet (in case of an active route)
  - …
- List a maximum of 3 different mid- or long-term actions be taken in the given scenario.
  - Ensure regular patching through respective management processes
  - Ensure regular security audits
  - Server hardening
  - Implement a Reverse Proxy / Web Application Firewall
  - Implement sensors such as NIDS, NIDS

  - ...

- Select an existing vulnerability of the "High" or "Medium" category on Mars and briefly describe how the chosen vulnerability can be closed.
  - Correct solution depends on the candidate's selected vulnerability and has to be assessed by the correction experts.