**Case Study**

Cyber security issues are continuing to grow at an alarming rate. With so many accessing the internet daily, the risk of online crime, stolen information, and exploitation is rising.

[Gelos Enterprises](https://share.tafensw.edu.au/share/items/d0b458dc-3922-409d-b1fe-9a2f785f4a38/0/?attachment.uuid=5f1677bf-8296-4137-ae33-8b9e30bad1ab), a leading Australian organisation that offers services to Australian businesses, has engaged with [DataTrust](https://share.tafensw.edu.au/share/items/22c51ecc-efca-455e-a7f2-18847749f30c/0/?attachment.uuid=7257a065-2c1f-4622-b2b2-9ee25ed654f9), a cyber security specialist company, undertake to assist with the management of cyber security on an ongoing basis.

You are the lead Penetration Tester working with DataTrust. DataTrust has informed Gelos about the latest vulnerability in the Gelos system. Your manager has tasked you to work with Gelos and test their system for the identified vulnerability. Your manager has asked you to conduct some initial research and complete a Penetration Testing Report as part of the quarterly cyber security testing schedule.

Your task as a lead Penetration Tester for DataTrust is to perform a network scan of all the devices on the Gelos network and identify the open ports on each device.

In case the scan output reveals an open port 80, you must utilise an enumeration tool such as gobuster or dirb to automatically conduct a web enumeration and identify any concealed directories that may exist.

Since this task requires repetitive work, you are expected to research and determine if automation of the process is possible and, if so, identify the most appropriate programming language to use.