

Cybersecurity: Technology and Governance

Audun Jøsang
1st edition 2024
Springer Nature



Exercises

Chapter 2: Threat actors, attack vectors, and malware

Problem 1: Attack vectors

- What is the most common attack vector for cyberattacks?
- How can deepfake voice and video be used in cyberattacks?
- How can USB devices such as (similar to) a USB flash drive be used to attack a computer?

Task 2: Supply chain attacks

- Explain what is meant by supply chain vulnerabilities.
- Describe examples of supply chain attacks that have occurred in recent years.
- What measures can a company take to reduce supply chain risk? (Cyber Supply Chain Risk Management, C-SCRM)?

Task 3: Botnet

- What is a botnet?
- What is a DDoS, and how can a botnet be used to do a DDoS attack?
- Mirai is a malware that was used to "take down" the internet in much of the United States through an attack on a Dyn DNS one day in October 2016. Briefly describe Mirai and how this attack was carried out

Task 4: XSS

You are a member of a new social platform called FAGSNAKK developed by and for students at the university where you can have academic discussions, organized with one page for each subject. One day, the FAGSNAKK page is full of the same dog picture that (it looks like) has been posted by various users (including you), without anyone remembering that they have done. A fellow student believes that this may be due to an XSS vulnerability in FAGSNAKK and that the images are the result of an XSS attack.

- What is an XSS attack?
- How could the XSS attack described above have been carried out?
- How could the attack on FAGSNAKK have been prevented?