1 Exercise 2.31: Translate into English

1.1 Щоби зробити недієздатним комп'ютер або навіть цілу мережу, хакери часто переповнюють мережу або маршрутизатори доступу фіктивним трафіком.

To disable a computer or even a whole network hackers often flood the network or the access routers with bogus traffic.

1.2 Крім того, щоби бути мішенню DoS-атаки, ваш комп'ютер може бути використаний для того, щоби розпочати DoS-атаку на іншу систему.

In addition to being the target of a DoS attack, your computer might be used to start a denial-of-service attack on another system.

1.3 Оскільки безпека сайтів в Інтернеті є взаємозалежною, ваш комп'ютер, навіть будучи кінцевою метою атаки, може становити загрозу для інших сайтів.

Since site security on the Internet is interdependent, your computer, even being an end target of an attack, could pose a threat to other sites.

1.4 Подібно до відомого давньогрецького міфу, комп'ютерний троянський кінь може відкрити зломлювачу легкий доступ до вашого комп'ютера.

Similar to a widely known Greek myth, a computer Trojan horse might allow the intruders to easily access your computer.

1.5 Важливо зазначити, що користуючись ненадійними сайтами, ви наражаєте свій веб-браузер на шкідливі сценарії.

It's important to note that by using untrustworthy sites you expose your computer to malicious scripts.

1.6 Більшість інцидентів, пов'язаних з комп'ютерною безпекою в мережі є наслідком застосування вірусів, хробаків, троянських коней та інших шкідливих та руйнівних кодів, за допомогою яких зломлювачі створюють безліч проблем власникам комп'ютерів.

Most network-related security incidents are a result of usage of viruses, worms, Trojan horses and destructive code, with which intruders create countless problems for computer owners.

1.7 Одним із негативних наслідків порушення безпеки є те, що зламані комп'ютери можуть використовуватися автоматично як стартові майданчики для атак на інші системи.

One of the negative implications of security breaches is how compromised computers might be automatically used as launching pads for attacking other systems.

1.8 Програми-лазівки дозволяють зломлювачу отримати віддалений доступ до вашого комп'ютера або заразити ваш комп'ютер вірусом чи змінити конфігурацію вашої системи.

Backdoor programs allow an intruder to gain remote access to your computer or infect your computer with a virus or change your system's configuration.

1.9 Комп'ютерні віруси, хробаки та троянські коні є тими засобами, за допомогою яких зломлювачі завдають шкоди безпеці інформаційної мережі у широкому масштабі.

Computer viruses, worms and Trojan horses are the tools with which intruders hurt a network's security on a large scale.

1.10 Часто хакери використовують інструментарій розподілених DoS-атак для того, аби порушити зв'язок між двома машинами або не дозволити суб'єктами отримати доступ до послуги.

Hackers often use distributed denial of service tools to disrupt the connection between two machines or prevent individuals from accessing a service.

1.11 Зломлювачі можуть вдаватися до різних пов’язаних з мережею дій з метою отримати контроль над домашніми комп’ютерами.

Intruders may resort to different network-related activities to gain control over your home computer.

1.12 Інформація, що становить комерційну таємницю на ризикує натрапити на аналізатори пакетів.

Proprietary information is at risk of being exposed to packet sniffers.