1. Modifikuj nasledovný text tak, aby tvrdenia boli správne.

E-mail predstavuje odosielanie správ z falošnej e-mailovej adresy alebo falšovanie e-mailovej adresy iného používateľa.

Útoky typu výpadok služby (Denial of Service) alebo dáta ako to robia nejaké iné typy útokov.

Cieľom DDoS útoku je nasýtiť sieťovú šírku pásma.

Útoky sociálneho inžinierstva na technologickú manipuláciu s počítačovým hárdverom alebo softvérovú zraniteľnosť a veľké technické znalosti.

vírusovej detekcie môže identifikovať nové vírusy alebo nové varianty existujúcich vírusov, tým že hľadá známy škodlivý kód, alebo obmenu takéhoto kódu v súboroch.

1. Vyznač pravdivé tvrdenia.

**x** DoS útok je úmyselný čin, ktorý spôsobuje znefunkčnenie počítača alebo siete (napr. zabraňuje používateľom prihlásiť sa do siete).

□ Adware je považovaný za nelegitímnu alternatívu ponúkanú zákazníkom, ktorí si neprajú platiť za softvér.

□ Napadnutie spyware-om negeneruje nechcenú aktivitu CPU, disku alebo nechcenú sieťovú prevádzku.

**x** Ak počítačový program vykoná akciu, ktorá úmyselne poškodí systém alebo dáta, nazývame ho škodlivý kód.

**x** Spoofing útok predstavuje to, keď sa zlomyseľná strana vydáva za iné zariadenie alebo za iného používateľa v sieti.

□ Útoky nultého dňa sú objavené počas niekoľkých minút.

1. Spoj termíny na ľavej strane s prislúchajúcimi definíciami na pravej strane

|  |  |  |
| --- | --- | --- |
| Dôvernosť |  | Zaistenie identity komunikujúcich subjektov. |
|  |  |  |
| Integrita dát |  | Prevencia neautorizovaného použitia zdroja. |
|  |  |  |
| Dostupnosť |  | Ochrana informácií pred sprístupnením neoprávneným osobám. |
|  |  |  |
| Autentifikácia |  | Včasný prístup  k informáciám. |
|  |  |  |
| Kontrola prístupu |  | Ochrana dát proti vytvoreniu, zmene, vymazaniu, zdvojovaniu alebo zmene poradia neoprávnenými osobami. |

1. Doplň čísla správnych tvrdení.

|  |
| --- |
| 2 |
| 4 |
| 5 |
| 7 |
|  |
|  |
|  |

**1** – Odmietnutie umožňuje jednotlivcovi zachovať právo kontrolovať, aké informácie o ňom sa zhromažďujú, ako sa používajú a kto ich používa.

**2** – Traffic padding je mechanizmus, ktorý vloží bity do medzier v dátovom toku, aby zmaril pokusy o analýzu sieťovej prevádzky.

**3** – Ochrana údajov sa vzťahuje k ochrane informácií od sprístupnenia neoprávneným subjektom.

**4** – Certifikácia je mechanizmus, ktorý používa dôveryhodné tretie strany, aby zabezpečili určité vlastnosti výmeny dát.

**5** – Polo-invazívne útoky môžu manipulovať s napadnutým zariadením, ale nerobia priamy elektrický kontakt s povrchom čipu.

**6** – Replikácia uzlov a spoofing sú príklady pasívnych útokov.

**7** – Jedna z ciest, ako spôsobiť pád systému je tá, že do vyrovnávacej pamäte vložíme viac dát, než je vyrovnávacia pamäť schopná udržať.