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

Ochrana dát je (voliteľný / nevyhnutný) (proaktívny / reaktívny) prístup na zamedzenie výpadku zákazníckych služieb, keď sú realizované nejaké modifikácie.

Sieťový bezpečnostný systém (je iba malá časť / je globálne riešenie) informačnej bezpečnostnej infraštruktúry organizácie.

Bezpečnostné služby sú implementované pomocou (bezpečnostných mechanizmov / bezpečnostných algoritmov) vzhľadom na bezpečnosť (protokolov / pravidiel).

Bezpečnosť (protokoly / mechanizmy) podporujú bezpečnostné služby a spúšťajú špecifické aktivity pre ochranu voči útokom.

(Všetky / Nie všetky) polo-invazívne alebo invazívne útoky sú aktívnymi útokmi.

(Všetky / Nie všetky) bezpečnostné hrozby sú ohrozením.

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

2. Označ pravdivé tvrdenia.

☐ Sieťová bezpečnosť sa zaoberá len bezpečnosťou v počítačoch na každom konci komunikácie.

☐ Zabezpečenie siete je rovnako dôležité ako zabezpečenie počítačov a šifrovanie správy.

☐ Bezpečnostný sieťový systém je sada hardvérových zariadení, ktoré sú použité a kryptografické algoritmy pre ochranu informačných a komunikačných systémov spoločnosti.

☐ Všetky bezpečnostné mechanizmy používajú kryptografické transformácie.

☐ Bezpečnostné mechanizmy sú rozdelené na tie, ktoré sú vykonávané v určitej protokolovej vrstve a tie, ktoré nie sú špecifické pre konkrétnu vrstvu protokolu alebo bezpečnostnú službu.

☐ Schopnosť útočníka je typicky určená jeho schopnosťami, tým čo zanechal po útoku a požadovanými nákladmi, ktoré minul pokiaľ ide o zariadenie.

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

3. Spoj termíny z ľavej strany s prislúchajúcou definíciou na pravej strane.

Vírus	Škodlivý softvér šírený prostredníctvom siete.
Červ	Javia sa ako bežné programy, ale môžu vykonávať akcie, ktoré užívateľ nemal v úmysle alebo si ich nebol vedomý.
Trojan	Softvér inštalovaný bez súhlasu užívateľa a slúži napr. na získanie informácií o správaní používateľa na webe.
Zombie	Samo-replikačné programy, ktoré nevyžadujú súbory k ich šíreniu.
Spyware	Samo-replikačné programy, ktoré používajú súbory na infikovanie a šírenie.

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

4. Doplň čísla správnych tvrdení z oblasti sieťových bezpečnostných hrozieb.

1 – Malvér je chybný softvér.

2 – Skener odkazuje na softvérový program, ktorý je používaný vzdialene hackermi na určenie možného zraniteľného miesta daného systému.

3 – Skenovací útok je, keď sa zlomyseľná strana vydáva za iné zariadenie alebo za iného používateľa v sieti.

4 – Niekedy môže mať antivírus nevýhodné vlastnosti a môže narušiť výkon počítača.

5 – Odstránením vírusu sa rozumie odstránenie kódu v infikovanom súbore, ktorý zodpovedá vírusu.

6 – Firewall je typický hraničný kontrolný mechanizmus alebo perimeter obrany.

7 – Niektoré systémy IDS len monitorujú a upozorňujú na útok, zatiaľ čo iné sa ho snažia zablokovať.

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).