1. Upravte následující text tak, aby jeho znění bylo pravdivé.

Pojmem e-mail označujeme proces odesílání zpráv z falešné (podvržené) e-mailové adresy či falšování e-mailové adresy jiného uživatele.

Útok typu DoS (*Denial of Service*) ani/a/ale uživatelská data, jak to některé jiné typy útoků dělají.

Hlavním cílem útoku typu DDoS je zcela vytížit dostupnou přenosovou kapacitu napadené sítě.

Útoky typu sociální inženýrství (*Social Engineering*) na přímém zneužití technické zranitelnosti počítačového hardwaru nebo softwaru a/ale určitou míru technických dovedností útočníka.

detekce virů umožňuje identifikovat i nové typy virů nebo nové varianty již existujících virů tím, že vyhledává známé části škodlivého kódu, či změny původního kódu v datových souborech.

1. Označte v následujícím textu pravdivá tvrzení.

**X** Útok typu DoS je úmyslným činem, který záměrně udržuje počítač nebo síť mimo provoz (například brání uživatelům v přihlášení se do sítě nebo do počítače).

□ Adware je považován za nelegitimní programovou alternativu pro spotřebitele (zákazníka), který nechce platit za legálně využívaný software.

□ Infiltrace větším množstvím spywaru nezpůsobuje nežádoucí aktivitu/vytížení procesoru (CPU), využívání kapacity pevného disku či generování nežádoucího síťového provozu.

**X** Počítačový program, který provádí činnost, která úmyslně poškozuje vlastní systém nebo uživatelská data je označován jako škodlivý kód (*Malicious Code*).

**X** Pojmem *Spoofing attack* je označováno zákeřné jednání jiného zařízení či osoby (skupiny zařízení či osob) využívající pro svou zlovolnou aktivitu dostupné síťové prostředky.

□ Útoky typu *Zero-day* jsou odhaleny během několika málo minut po jejich začátku.

1. Přiřaďte správnou položku z levého sloupce odpovídajícímu popisu uvedenému v pravém sloupci.

|  |  |  |
| --- | --- | --- |
| Důvěrnost (*Confidentiality*) |  | Zajišťuje totožnost komunikujících subjektů. |
|  |  |  |
| Úplnost dat (*Data Integrity*) |  | Prevence neoprávněného využití dostupných prostředků. |
|  |  |  |
| Dostupnost (*Availability*) |  | Ochrana informací (dat) před prozrazením neoprávněným osobám. |
|  |  |  |
| Ověření identity (*Authentication*) |  | Možnost včasného přístupu k informacím. |
|  |  |  |
| Kontrola oprávnění přístupu (*Access Control*) |  | Ochrana dat proti jejich neoprávněnému vytváření, změně, vymazání, duplikování nebo reorganizování neoprávněnými osobami. |

1. Doplňte do následující tabulky čísla pravdivých tvrzení.

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

**1** – Průkaznost (*Non-repudiation*) umožňuje zachování individuálního práva kontrolovat, jaké informace jsou o daném subjektu shromažďována, jakým způsobem jsou využívána a kdo tyto informace je oprávněn používat.

**2** – Provozní výplň (*Traffic Padding*) je mechanismus, který záměrně vkládá bity do mezer v datovém toku tak, aby efektivně zmařil možné pokusy o analýzu síťového provozu.

**3** – Ochrana údajů se obecně vztahuje k ochraně informací omezující jejich vyzrazení neoprávněným osobám či subjektům.

**4** – Certifikované ověření (*Notarization*) je mechanismus, který využívá služeb důvěryhodné třetí strany k nastavení určitých vlastností a parametrů pro bezpečnou výměnu dat.

**5** – Semiinvazivní typ útoku umožňuje koordinovanou manipulaci s napadeným zařízením, ale neumožňuje přímý elektrický kontakt s integrovanými obvody, které jsou jeho součástí.

**6** – Replikace uzlů a spoofing jsou příklady pasivních typů útoků.

**7** – Havárii systému je možné vyvolat přetížením vyrovnávací paměti, kdy objem ukládaných dat je výrazně vyšší než kolik jich je schopna vyrovnávací paměť pojmout.