**Zadanie 2.**

Zaznacz jedną poprawną odpowiedź:

**1. Robak to:**

 wirus komputerowy, który potrafi dołączyć się do istniejącego programu komputerowego,

 wirus komputerowy, który uaktywnia się, gdy nadejdzie odpowiednia data,

 wirus komputerowy, który rozsyła pełne kopie samego siebie w sieciach,

 wirus komputerowy, który uaktywnia się, gdy użytkownik zainfekowanego komputera uruchomi jakiś program.

**2. Koń trojański to:**

 wirus komputerowy, który udaje przydatne oprogramowanie, uaktywnia się, gdy użytkownik zainfekowanego komputera uruchomi jakiś program,

 wirus komputerowy, który uaktywnia się, gdy nadejdzie odpowiednia data,

 wirus komputerowy, który ma zdolność samoreplikacji,

 wirus komputerowy, który potrafi dołączyć się do istniejącego programu komputerowego,

**3. Bomba logiczna to:**

 wirus komputerowy, który potrafi dołączyć się do istniejącego programu komputerowego,

 wirus komputerowy, który uaktywnia się, gdy nadejdzie odpowiednia data, lub zostanie spełniony inny warunek,

 wirus komputerowy, który rozsyła pełne kopie samego siebie w sieciach,

 wirus komputerowy, który ma zdolność samoreplikacji.

**4. Głównym zadaniem zapory sieciowej (ogniowej) jest:**

 naprawianie wirusów,

 szukanie wirusów w systemie,

 usuwanie wirusów,

 niedopuszczanie, aby wirusy weszły do systemu.

**5. Głównym zadaniem programu antywirusowego jest:**

 zabezpieczanie przed wejściem wirusów do systemu,

 naprawianie wirusów,

 znajdowanie i usuwanie wirusów,

 zamrażanie plików lub programów zarażonych wirusem.

**6. Makrowirus to:**

 wirus komputerowy, który potrafi dołączyć się do istniejącego programu komputerowego,

 wirus komputerowy, który uaktywnia się, gdy nadejdzie odpowiednia data, lub zostanie spełniony inny warunek,

 wirus komputerowy, który rozsyła pełne kopie samego siebie w sieciach,

 wirus komputerowy, który ma zdolność samoreplikacji, do czego wykorzystuje języki makr zawarte w zarażonym środowisku.

**7. Exploit to:**

 jeden ze sposobów zwiększania wydajności systemu,

 wirus zapoczątkowujący reakcję łańcuchową w sieci WAN,

 czujnik reagujący na pojawienie się wirusa,

 program wykorzystujący błędy w oprogramowaniu do przejęcia kontroli na komputerem.

**8. Phishing to:**

 wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję,

 skanowaniu dysku połączone z kasowaniem wirusów,

 czyszczenie jądra systemu podczas uruchamiania komputera,

 stała kontrola antywirusowa działająca w tle.

**9. Keylogger to:**

 program podpowiadający hasła zapisane w systemie,

 program przechwytujący kody wciskanych klawiszy,

 klucz szyfrujący dane aktualnie zalogowanego użytkownika,

 zabezpieczenie przez zalogowaniem się do uśpionego systemu.

**10. Spyware:**

 programy, których celem jest szpiegowanie działań użytkownika,

 tymczasowe ukryte pliki internetowe pozostające w buforze,

 uszkodzone pliki typu „cookies” pozostające po surfowaniu,

 niepotrzebne wpisy w rejestrach systemu (śmieci).

**11. Rootkit:**

 włączenie dźwięków, które są przy uruchamianiu systemu operacyjnego,

 zestaw programów do odwirusowywanie komputera,

 program ukrywający niebezpieczne pliki i procesy przed użytkownikiem i oprogramowaniem antywirusowym,

 narzędzie do porządkowania dysku.

**12. Backdoor to:**

 program blokujący porty komputera przez nieuprawnionym dostępem,

 sprzętowe zabezpieczenie komputera,

 mechanicznie zabezpieczona tylna ścianka komputera,

 luka w zabezpieczeniach tworzona umyślnie w celu późniejszego wykorzystania przez włamywacza komputerowego.

**13. Komputer zombi to:**

 jeden z komputerów w sieci wyłapujący uszkodzone pakiety,

 komputera bez klawiatury i monitora pełniący rolę bramy,

 komputer, w którym bez wiedzy jego posiadacza zainstalowano program sterowany przez osobę z zewnątrz,

 potoczne określenie komputera przestarzałego, który powoduję nadmiarowy ruch w sieci.

**14. Atak DoS:**

 bombardowanie serwera powodujące przeciążeniu aplikacji którejś z oferowanych przez niego usług,

 regularne wysyłanie listów zawierających wirusy,

 atak mający na celu złamanie zapory ogniowej,

 działanie polegające na wywołaniu szybkich zmian napięcia w sieci elektrycznej mające na celu destabilizację komputera.

imię i nazwisko oraz klasa