ТЕСТ
ЗА ОЦЕНКА НА ЗНАНИЯТА ПО ДИСЦИПЛИНА
„СИСТЕМИ ЗА СИГУРНОСТ“

Забележка: **Въпросите от 1 до 20 могат да имат повече от един верен отговор.**

Въпрос № 1: ***Политиката за мрежова и информационна сигурност е:***

а) намерения за организиране на защитата на обработката, съхранението и разпространението на информацията

б) набор от нормативни документи, правила и норми за поведение, които определят как организациите защищават обработката, съхранението и разпространението на информацията

в) въвеждане на система за управление на мрежовата и информационна сигурност

Въпрос № 2: ***Принципът на „най-слабо звено”е концепция, при която:***

а) се наблюдават и елиминират звената с най-слаба устойчивост на интервенции или с наличие на възможност за проникване;

б) се търсят най-слабите звена в системата с цел незаконно проникване

в) се слагат защитни средства пред най-слабото звено

Въпрос № 3: ***Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалността, ако***:

а) се осъществи нерегламентиран достъп от трети лица

б) съобщенията не достигнат до адресата

в) се случи разрушаване на съобщението

Въпрос № 4: ***«Разпределена атака от типа отказ за обслужване» е:***

а) атака, която цели прихващането на пароли и друга конфиденциална информация

б) атака, която цели нерегламентиран достъп до информационни ресурси

в) атака, при която сървърът на системата получава едновременно огромно количество пакети за обслужване от «зомбирани» компютри, разположени по целия свят

Въпрос № 5: ***Нов цикъл на оценка на риска се предприема, ако:***

а) препоръчваните мерки за сигурност са свързани с големи разходи

б) изчислените вероятности за настъпване на инцидент са твърде високи

в) остатъчният риск не удовлетворява ръководството на организацията.

Въпрос № 6: ***Виртуални частни мрежи за отдалечен достъп се изграждат чрез използване на:***

а) протоколът Internet Protocol Security (IPSec);

б) протоколът Secure Socket Layer (SSL) (или модернизирания му вариант Transport Layer Security (TLS));

в) и двата посочени протокола.

Въпрос № 7: ***Сертификацията на програмни продукти и информационни системи относно информационната сигурност се провежда съгласно международния стандарт:***

а) ISO/IEC 27001;

б) ISO/IEC 15408 (Common Criteria);

в) ISO/IEC 17024

Въпрос № 8: ***Защитата срещу нежелан софтуер в информационните системи се осъществява чрез:***

- ***забрана за използване на нерегламентиран софтуер;***
- ***използване на антивирусен софтуер и софтуер за откриване на нерегламентирани промени на информационните активи.***

а) вярно е само първото;

б) вярно е само второто;

в) верни са и двете.

Въпрос № 9: ***Посочете коя от тези организации е ангажирана със стандартизация в областта на мрежовата и информационна сигурност:***

а) Международен съюз по далекосъобщения;

б) Internet Engineering Task Force;

в) Европейска агенция по мрежова и информационна сигурност.

Въпрос № 10: ***Центърът за действие при кризисни ситуации в компютърната сигурност предлага:***

а) бърза и ефективна реакция срещу атаките и заплахите, свързани със сигурността, с цел осигуряването на добре защитена информационна среда;

б) съхраняване на критични данни с цел тяхното възстановяване след инцидент с компютърната сигурност;

в) консултантски услуги относно програмни продукти за защита на информационни активи.

Въпрос № 11: ***Откриването на опити за проникване от IDS/IPS, базирано на аномалии се извършва:***

а) чрез сравняване на сигнатури по време на наблюдаваните събития за идентифициране на възможни инциденти;

б) чрез сравняване на дефиниции на дейност, които се считат за нормални с наблюдаваните събития за идентифициране на значителни отклонения;

в) сравняване на предварително определени профили на общоприети дефиниции на доброкачествена протоколна дейност за всяко протоколно състояние при наблюдаваните събития, за да се идентифицират отклонения.

Въпрос № 12: ***Технологията DNSSEC:***

а) реализира създаването на виртуални частни мрежи;

б) защищава сървърите от неоторизиран достъп;

в) определя процес, при който подходящо конфигуриран сървър на имената може да провери автентичността и целостта на резултатите от заявките от подписана зона.

Въпрос № 13: ***Инфраструктурата на публичния ключ се базира на:***

а) блокови шифри;

б) поточни шифри;

в) асиметрични шифри

Въпрос № 14: ***Зоните за сигурност контролират трафика за да се гарантира, че:***

а) на изисквания трафик е разрешено да премине между зоните;

б) злонамереният трафик се идентифицира и се филтрира, където е възможно;

в) трафикът е насочен към специфицираните ресурси.

Въпрос № 15: ***Основните цели на управлението на уязвимости са:***

а) идентифициране и коригиране на грешки в софтуера, които могат да повлияят на сигурността, производителността и функционалността;

б) увеличаване на устойчивостта на софтуера;

в) изменяне на функционалността или преадресиране на заплахата за сигурността.

Въпрос № 16: ***Trouble ticket (или доклад за авария)*** **е:**

а) предупреждение за евентуална опасност;

б) механизъм за описание на инцидента по унифициран начин, така че да се осигури неговото идентифициране, докладване, отработване и решение;

в) доклад за направена проверка на факторите на сигурността.

Въпрос № 17: ***Препоръката на ITU X.1500 (CYBEX) регламентира:***

а) рамката за обмен на информация относно кибер-сигурността;

б) съдържанието на сертификата за електронен подпис;

в) методите за контрол на достъпа.

Въпрос № 18: ***Посочете кои от следващите принципи са заложени в държавната политика по мрежова и информационна сигурност:***

а) минимална привилегия;

б) максимална отговорност;

в) точка на запушване.

Въпрос № 19: ***Nessus е продукт за:***

а) откриване на нетипичен трафик в мрежата;

б) изчерпателно тестване на уязвимости;

в) докладване на инциденти.

Въпрос № 20: ***Разделянето (сегрегацията) на мрежите*** **е:**

а) метод за физическа защита на мрежите от външни въздействия;

б) метод за увеличаване пропускната способност на мрежата.

в) метод за контрол на сигурността на големи мрежи чрез разделяне на отделни логически домейнни мрежи, определени въз основа на оценка на риска и различните изисквания за сигурност в рамките на всеки един от домейните.

Въпрос № 21: ***Посочете основополагащ документ на Международния съюз по далекосъобщения (ITU), свързан с кибер-сигурността***

……
……
……
……

Въпрос № 22: ***Посочете трите основни съставляващи на мрежовата и информационна сигурност***

……
……

Въпрос № 23: ***Посочете основните стъпки при оценката на риска***

……
……
……

Въпрос № 24: ***Посочете разликите между IDS и IPS технологиите***

……
……
……
……

Въпрос № 25: ***Какво представлява „хеш-функцията“?***

……
……
……

Въпрос № 26: ***Какво представлява тестването за проникване?***

……
……
……

Въпрос № 27: ***Какво представлява защитната стена (firewall)?***

……
……

Въпрос № 28: ***Какво е инцидент с компютърната сигурност?***

……
……
……

Въпрос № 29: ***Какво представлява Honeypot?***

……
……
……
……

Въпрос № 30: ***Какво е Security Content Automation Protocol (SCAP)?***

……
……
……
……