Безпека інформаційних і комунікаційних систем

Усього балів 15/20

спец. 125 "Кібербезпека", ОПП "Безпека інформцаійних і комунікаційних систем"

✓ Яка криптографічна технологія використовується IPSec для автентифікації повідомлень на основі хеш-функцій? 1/1

- ○ Шифрування RSA
- ◉ HMAC ✓
- ○ Алгоритм Діффі-Хеллмана

✓ Яке значення протоколу керування з’єднанням (LCP) у протоколі «точка-точка» (PPP)? 1/1

- ◉ Встановлює та розриває з’єднання «точка-точка» ✓
- ○ Керує протоколами мережевого рівня
- ○ Шифрує пакети даних

✗ Які функції виконує інкапсуляція пакетів у технології тунелювання? 0/1

- ○ Захист конфіденційності вмісту пакету
- ◉ Приховання мережевої структури між точками ✗
- ○ Запобігання конфліктам адрес між локальними мережами

Правильна відповідь

- ◉ Захист конфіденційності вмісту пакету

✓ Який із наведених нижче протоколів спеціально розроблено для створення захищених віртуальних каналів для віддалених користувачів, які отримують доступ до локальних мереж через Інтернет? 1/1

- ○ PAP
- ○ SET
- ◉ PPTP ✓

✓ Яка основна перевага використання таких протоколів, як PPTP, L2F і L2TP, для безпечного тунелювання на канальному рівні? 1/1

- ○ Сумісність лише з IP-протоколами
- ◉ Можливість інкапсулювати кілька протоколів мережевого рівня ✓
- ○ Розширені можливості шифрування

✗ Який протокол автентифікації забезпечує захист від атак повторного відтворення та взаємної автентифікації клієнт-сервер у реалізаціях PPTP? 0/1

- ○ PAP
- ○ MSCHAP
- ◉ EAP-TLS ✗

Правильна відповідь

- ◉ MSCHAP

✗ Яка основна роль протоколу Microsoft Point-to-Point Encryption (MPPE) у реалізаціях PPTP? 0/1

- ◉ Управління обміном ключами ✗
- ○ Динамічний вибір довжини ключа
- ○ Маршрутизація пакетів даних

Правильна відповідь

- ◉ Динамічний вибір довжини ключа

✗ Яка основна функція протоколу обміну ключами в Інтернеті (IKE) в IPSec? 0/1

- ○ Обробка шифрування пакетів
- ◉ Управління асоціаціями безпеки ✗
- ○ Автентифікація користувачів

Правильна відповідь

- ◉ Автентифікація користувачів

✓ Яке визначення «доступу» в контексті інформаційних систем? 1/1

- ◉ Взаємодія між ресурсами системи ✓
- ○ Шифрування даних
- ○ Видалення інформації

✓ Як зазвичай здійснюється автоматичний несанкціонований доступ? 1/1

- ○ З втручанням людини
- ◉ Використання спеціалізованого програмного забезпечення ✓
- ○ Через фізичне втручання

✓ Чим пасивний неавторизований доступ відрізняється від активного неавторизованого доступу? 1/1

- ○ Пасивний доступ передбачає пряме маніпулювання ресурсами
- ○ Активний доступ залежить від втручання людини
- ◉ Пасивний доступ не впливає безпосередньо на ресурси ✓

✓ Який тип несанкціонованого доступу використовує існуючі недоліки політики безпеки? 1/1

- ○ Активне підслуховування
- ◉ Постполітизований доступ ✓
- ○ Пасивне постукування

✓ Що з наведеного є функцією міжмережного екрану? 1/1

- ○ Дублювання даних
- ○ Стиснення даних
- ◉ Аналіз потоку даних ✓

✓ Яке призначення екранувального шлюзу прикладного рівня? 1/1

- ◉ Фільтрація пакетів додатків ✓
- ○ Фільтрація фізичних даних
- ○ Фільтрація транспортних даних

✓ Яка властивість системного ресурсу дозволяє користувачеві з відповідними дозволами використовувати його відповідно до правил політики безпеки без тривалого очікування? 1/1

- (●) Доступність ✓
- ( ) Цілісність
- ( ) Конфіденційність

✓ Який вид аутентифікації вирішує завдання встановлення дійсності ідентифікатора, запропонованого суб'єктом взаємодії? 1/1

- ( ) Автентифікація об'єкта
- (●) Автентифікація суб'єкта ✓
- ( ) Автентифікація даних

✓ Які основні напрями захисту інформаційних ресурсів визначає політика безпеки? 1/1

- ( ) Шифрування, розшифрування, приховування інформації
- ( ) Функціональність, надійність, адаптованість, ергономічність, економічність
- ( ) Створення, удосконалення, упорядкування, взаємодія компонентів системи
- (●) Нормативно-правові, організаційні, апаратні, програмні, криптографічні, стеганографічні ✓

✓ Які методи можуть застосовуватися для автентифікації суб'єкта? 1/1

- (●) Автентифікація з нульовим розголошенням, симетричні та асиметричні методи ✓
- ( ) Автентифікація з нульовим розголошенням, шифрування даних, контроль доступу
- ( ) Симетричні методи, асиметричні методи, правила розмежування доступу
- ( ) Шифрування даних, контроль доступу, перевірка дозволу на користування

✓ Які кроки важливі для ефективного контролю доступу до інформації? 1/1

- ( ) Визначення рівня доступу, надання прав доступу в письмовому вигляді, перевірка дозволу на користування системою
- ( ) Фіксування випадків успішного і безуспішного доступу, встановлення рівня доступу, перевірка дозволу на користування
- (●) Перевірка ідентичності претендента, встановлення відповідності між об’єктом і його ідентифікатором, контроль за доступом користувачів і процесів ✓

✗ Які вимоги повинні задовольняти міжмережні екрани для забезпечення безпеки? 0/1

- ( ) Аналіз та реєстрація подій, перевірка дійсності переданих даних
- ( ) Ідентифікація та аутентифікація користувачів
- ( ) Фільтрація повідомлень, трансляція внутрішніх мережних адрес
- (●) Висока якість, керованість і гнучкість, продуктивність і прозорість, самозахищеність ✗

Правильна відповідь

- (●) Фільтрація повідомлень, трансляція внутрішніх мережних адрес