Лекція 1

Доступність- можливість отримати інформаційну послугу.

Цілісність- актуальність інформації, її захищеність.

Конфіденційність-захищеність від несанкціонованого ознайомлення.

Кібербезпека-стан захищеності кіберпростору від ризику стороннього впливу, своєчасне виявлення.

Інцидент- події, що полягають в реалізації загрози.

Можна здійснити через:

* Несанкціонований доступ
* Втручання в дані
* Втручання в роботу системи
* Втручання в мережу
* Незаконне використання обладнення

Лекція 2

Якщо було зафіксовано порушення кібербезпеки на ОІД(об’єкт інформаційної діяльності), потрібно вжити таких заходів:

* Ідентифікувати інцидент
* Локалізувати область ІТ-інфраструктури
* Обмежити доступ до задіяного в інциденті
* Повідомити підрозділ інформбезпеки
* Залучити компетентних фахівців
* Скласти план дій, вести записи щодо роботи
* У присутності 3 особи вилучити та опечатати носії з доказовою базою (оформити протоколи, зняти відео, опис об’єктів, зберегти все в надійному місці)
* Відновити інформаційну систему
* Скласти звіт з достовірними доказами

**ISO**- міжнародна організація, яка займається ратифікацією стандартів(надання їм юридичної сили)

Новий стандарт ISO : 27037

Лекція 3

Кібератака- напад з урахуванням всіх вразливостей, щоб порушити конфіденційність.

Категорії кібератак:

* Information gathering
* Unauthorized access attempts
* Denial of service
* Suspicious activity
* System attack

Кібертероризм- ПОЛІТИЧНО вмотивовані кібератаки, які мали план з використанням високих технологій.

Лекція 4

**ISACA**-(information system audit and control association) – всесвітня організація з розробки методологій та стандартів в галузі управління, безпеки ІТ

!!! INFORMATION SECURITY !!!

ASSET MANAGEMENT: управління активами компаній, захист конф. оп.

RISK MANAGEMENT: управління ризиками, передбачуваність загроз.

BUSINESS CONTINIUTY/ DISASTER RECOVERY: продовження роботи в разі інциденту, відновлення даних.

RULES OF BEHAVIOR: правила опрацьовування даних, аналіз поведінки в критичних ситуаціях.

COMPLIANCE: побудова та відповідність виконуваних операцій згідно з світовими стандартами.

ACQUTION/DEVELOPMENT/MAINTANCE: ЛІЦЕНЗІЙНЕ програмне забезпеч.

COMMUNICATIONS AND OPERATIONS: здійснення фінансових та інф. операцій з використанням криптологічних методів захисту даних, виготовлення/зміна паролів.

VENDOR MANAGEMENT: система аналізу роботи з постачальником, моніторинг досягнень для операційного оновлення.

**DNS**- система доменних імен. Містить базу даних публічних ІР і пов’язаних з ним хостів. Перекладає імена хостів в ІР.

Інтернет периметр повинен:

* Прокладати трафік між підприємництвом і інтернетом
* Не допускати запущеня файлів через HTML
* Контролює мережеві порти
* Виявляє, блокує заражений мережевий трафік
* Усуває спами , віруси, інше
* Фільтрує сайти

Для VPN повинен

* Припинити трафік від віддалених користувачів
* Припинення для користувачів, що набирають номер
* Віддалений користувач може зайти тільки через аутентифікацію

Для WAN повинен

(комп'ютерна мережа, що охоплює величезні території, мільйони комп'ютерів). Для порівняння, Персональна мережа, Локальна мережа (LAN) зазвичай не виходять за межі будівлі)

* Шифрування даних за бажанням
* Блокування небажаних трафіків

Лекція 5

Policies(Standarts)- документ з правилами про необхідні чи заборонені дії.

Procedures-детальна інфа про те, як дотримуватись політиків.

Guidelines-(керівні принципи)- загальні вказівки, як і що робити в оремих ситуаціях, виняткових.

OSI-модель, яка описує, як мають взаємодіяти мережеві протоколи і обладнання

OSI LAYERS

APPLICATION: посередництво між програмними програмами і іншими рівнями мережевих служб. Тобто з поста в app.l/з в app.l з заданим форматом в пост.

PESENTATION: формати, шифрування, стиснення даних

SESSION: координує та керує з’єднаннями користувачів. Це рівень, відповідальний за відкриття та закриття зв’язку між двома пристроями. Час між відкриттям і закриттям називається сеансом. Сеансовий рівень гарантує, що сеанс залишається відкритим достатньо довго для передачі всіх даних, а потім негайно закриває сеанс, щоб уникнути марної витрати ресурсів.

TRANSPORT: забезпечує надійну, послідовну передачу даних, виконує контроль помилок, запитуючи повторну передачу, якщо це не так. МІЖМЕРЕЖНИЙ

NETWORK: перекладає адреси, мережевий рівень також знаходить найкращий фізичний шлях для досягнення даними місця призначення; це відомо як маршрутизація.

DATA LINK: поділяє дані на фрейми. ВНУТРІШНЬОМЕРЕЖНИЙ, відповідає за контроль потоків і помилок у внутрішньомережевому зв’язку, МІЖ ДВОМА ПРИСТОРЯМИ В ОДНІ МЕРЕЖІ.

PHYSICAL: керує сигналами між мережевими cистемами на фізичному рівні. Тобто кабелі і комутатори.

TCP/IP-набір протоколів, що використовується, як стандарт. Орієнтовані на мережу.

Лекція 6

Основні загрози безпеки інформації: незаконні:

* Розкриття
* Обмін
* Використання
* Використання

Компрометація інформації- коли стороння особа має доступ до неї, і має можливість змінювати дані.

Використання ресурсів локальної обчислювальної мережі- навіть не торкаючись користувацьких данів/інфи. Можна нанести збитки.

Лекція 7

Фаєрвол-межа між мережами. Зазвичай між відкр. і зак.. захист інфи, блокування акат з зовнішнього середовища.

IDS-система виявлення вторгнень

VPN-віртуальна приватна мережа. Прозоре для користувача з’єднання локальних мереж , зберігаючи конф, ціл. завдяки шифруванню.

Фаєрвол(брандмауер) дозволяє:

* Блокувати доступ до сайтів
* Обмеження трафіку у сегментів громадських послуг
* Запобігає доступу певних осіб до певних серверів
* Моніторинг та запис зв’язку між внутрішніми і зовнішніми мережами.
* Шифрування , створюючи VPN

Атаки на брандмауери:

* Підробка ІР файлів(ІР спуфінг) підроблене проходить базу правил брандмауера, проникнення через периметр
* Специфікація маршрутизації джерела- визначення маршруту, що обходить брандмауер
* Мініатюрна атака фрагментів – зловмисник надсилає розбиті на частинки ІР пакети з надією…

Лекція 8

VLAN-віртуальні локальні мережі(групи логічно сегментованих лок.мер)

DMZ-демілітаризована зона-локальна мережа, що є у компанії, мережа приватних компів, дмз встановлює зону безпеки, брандмауер

Лекція 9

IDS-cистема виявлення вторгнень

IPS-розшишення ідс

Ключові елементи криптографічних систем:(ключ, його довжина, шифр)

2 типи криптограф. систем:

1. Симетричні (одиночні, двонаправлені)
2. Асиметричні(пари ключів, один секретний, інший загальнодоступний)

Система відкритого ключа (PKI)- правила ідентичності.

DES-стандарт шифрування даних 64 біт

Digital cer.-засвідчує справжність власника відкритого ключа

Certificate authority- орган в мережі, що перевіряє запит цифрового сертифікату і повідомляє ЦС видавати його

Лекція 10

Цифрові сертифікати - складається з відкритого ключа та ідентифікаційної інформації про власника відкритого ключа.

IPSec - використовується для зв'язку між двома або більше хостами та підмережами. Встановлює VPN за допомогою шифрування транспорту та тунелю.

(Secure Sockets Layer, SSL) та (Transport Layer Security, TLS) - це криптографічні протоколи, що забезпечують безпечну комунікацію в Інтернеті.

SET - це протокол для захисту платіжних операцій між усіма учасниками транзакцій з кредитними картками

Лекція 10

Тестування на проникнення включає виявлення наявних уразливостей, а потім використання загальних методів експлуатації для:

• Підтвердження захищеності

• Оцінити рівень ефективності та якості існуючих засобів безпеки

• Визначити, як конкретні вразливості піддають ІТ-ресурсам та активам

• Забезпечення відповідності стандартам

Фази тестування на проникнення:

* Планування- На етапі планування встановлюються цілі, визначається сфера застосування та тест затверджується та документується керівництвом.
* Виявлення(Discovery:)- На етапі відкриття тестувальник проникнення збирає інформацію, проводячи дослідження організації та скануючи мережі для виявлення портів та служб. Методи: Випробовування DNS, WHOIS-запити. Пошук веб-серверів для імен співробітників та контактної інформації .На етапі виявлення також проводиться оцінка вразливості.
* Атака-Фаза атаки - це процес перевірки раніше виявлених уразливостей шляхом спроби їх використання.
* Звітність(Reporting)- Фаза звітування відбувається одночасно з іншими фазами

Управління мережею - це процес оцінки, моніторингу та підтримки мережевих пристроїв та з'єднань.

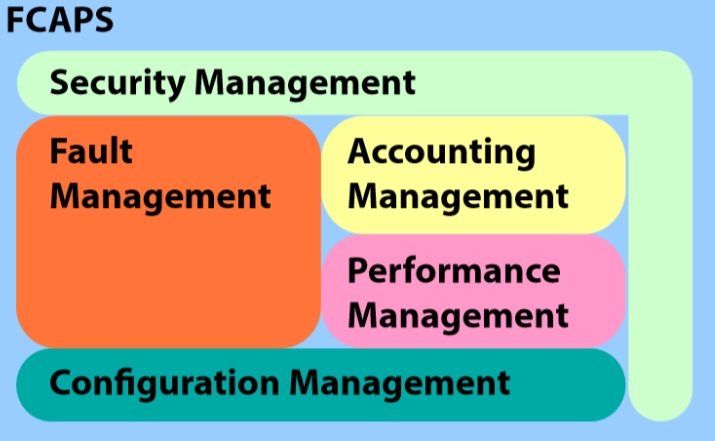
• Управління відмовами(Fault Management) - виявляє, виділяє, повідомляє та виправляє несправності, що виникають у мережі.

. • Управління конфігурацією(Configuration Management) - включають управління файлами конфігурації, запасами та програмним забезпеченням.

• Управління обліком(Accounting Management) - інформація про використання мережевих ресурсів.

• Управління продуктивністю(Performance Management) - відстежуйте показники ефективності. Сюди входить час відповіді, використання посилань та показник помилок.

• Управління безпекою(Security Management) - надайте доступ до мережевих пристроїв та корпоративних ресурсів уповноваженим особам. Ця категорія зосереджена на автентифікації, авторизації, брандмауерах, сегментації мережі, IDS та сповіщеннях про спроби порушення.



LAN

ризик, пов’язаний із використанням локальних мереж, включає:

• втрату цілісності даних та програм через несанкціоновані зміни;

• відсутність поточного захисту даних

• Вірус та зараження глистами

• Неправильне розкриття даних через загальний доступ, а не необхідність знати положення доступу; Порушення ліцензій на програмне забезпечення шляхом використання неліцензованих програмного забезпечення.

Користувач LAN

• прослуховування внутрішнього користувача

• перенастроювання мережевої адреси для того, щоб претендувати на іншу адресу

• знищення журналу та аудит даних Доступні положення безпеки LAN залежать від програмного продукту, версії продукту та реалізації.

Загальнодоступні адміністративні можливості мережевої безпеки включають:

• оголошення власності на програми, файли та сховище.

• Обмеження доступу до основи лише для читання.

• Реалізація запису та блокування файлів.

• Забезпечення процедур входу в систему для ідентифікації користувача / пароля та частоти зміни.

• Використання комутаторів для реалізації політики безпеки порту. Це запобіжить підключенню до локальної мережі несанкціонованих хостів з невідомими адресами.

• Шифрування локального трафіку за допомогою IPSec (IP-безпеки) протоколу.

Порт - це логічне з'єднання

Тср.ір позначаючи порт - це спосіб, яким клієнтська програма визначає конкретну серверну програму на комп'ютері в мережі. номер порту - це спосіб ідентифікувати конкретний процес, до якого слід пересилати Інтернет при надходженні на сервер.

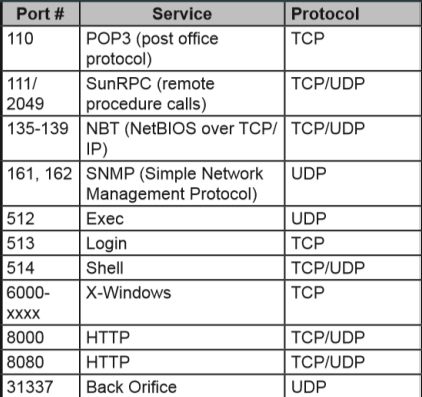
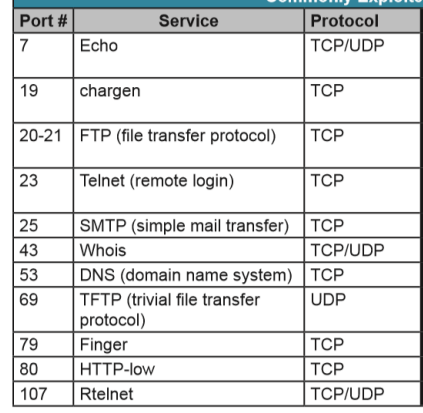
Допустимі номери портів становлять від 0 до 65535. Порти від 0 до 1023 зарезервовані для певних пільгових послуг - відомих портів. Наприклад, для послуги HTTP порт 80 визначається як за замовчуванням

IANA перераховують зареєстровані номери портів:

• Відомі порти від 0 до 1023: Контрольовані та призначені IANA, можуть використовуватися лише root системними процесами, що виконуються привілейованими користувачами.

• Зареєстровані порти - від 1024 до 49151: в більшості систем можуть використовуватися звичайні користувацькі процеси або програми, виконані звичайними користувачами.

•Динамічні та / або приватні порти від 49152 до 65535: IANA не перерахована через їх динамічний характер.



Тунелювання - це процес інкапсуляції одного типу протоколів в інший

Два поширених типи тунелювання включають:

• протокол тунелювання "точка-точка" (інкапсулює дані протоколу "точкаточка". Він простий, але менш безпечний, ніж інші протоколи тунелювання.

• Протокол тунелювання рівня 2 (L2TP) - протокол, який інкапсулює дані протоколу "точка-точка" і сумісний між обладнанням різних виробників. Кінцеві точки не повинні розташовуватися в одній мережі і можуть залишатися ізольованими від іншого трафіку

Будь-який VoIP-пристрій є пристроєм IP; отже, він вразливий до тих же типів атак, що і будь-який інший IP-пристрій. ГОЛОСОВЕ

Ризик віддаленого доступу включає:

• DoS, коли віддалені користувачі можуть не мати можливості отримати доступ до даних або додатків;

• Зловмисні треті сторони, які можуть отримати доступ до конфіденційні дані, використовуючи слабкі місця в мережевих протоколах

• Неправильно налаштоване комунікаційне програмне забезпечення, що може призвести до несанкціонованого доступу або модифікації інформацій

• Неправильно налаштовані пристрої в корпоративній обчислювальній інфраструктурі

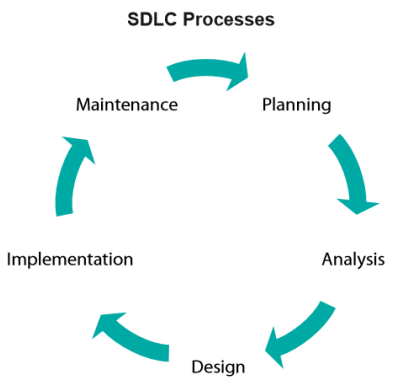
• Хост-системи не захищені належним чином, що може бути використане зловмисник отримує доступ дистанційно

• Проблеми фізичної безпеки на комп’ютерах віддалених користувачів

Управління віддаленим доступом включає:

• Політику та стандарти • Правильні авторизації • Механізми ідентифікації та автентифікації • Інструменти та методи шифрування, такі як використання VPN • Система та мережеве управління.

Життєвий цикл розвитку системи (SDLC, System Development Life Cycle)



SDLC включає: • ІТ-процеси для управління та контролю проектної діяльності • Мета для кожної фази життєвого циклу • Поступові кроки або результати

Зокрема, SDLC є формальним процесом для характеристики вимог до проектування і повинен включати: • бізнес-вимоги, описи того, що повинна робити система; • функціональні вимоги та використання кейсів, що описують взаємодію користувачів із системою; • технічні вимоги, інформаційні критерії, яким система повинна відповідати • Вимоги щодо зменшення ризику та контролю для захисту цілісності системи.

Тестування Фаза тестування SDLC включає: • Перевірку та перевірку того, що програма, підсистема чи додаток та розроблені засоби безпеки виконують функції, для яких вони були розроблені; інші компоненти системи • Визначення того, чи працюють блоки, що випробовуються, без будьяких несправностей або негативного впливу на інші компоненти системи. • Різноманітні методики розробки та організаційні вимоги для забезпечення широкого спектру схем або рівнів тестування З точки зору безпеки, це повинно включати тестування вразливості та контролю

Ін'єкція (Injection) недоліки виникають, коли ненадійні дані надсилаються перекладачеві

Зламана автентифікація та управління сесіями (Broken Authentication and Session Management) Якщо функція не виконана належним чином, вона може дозволити зловмиснику компрометувати парол

Міжсайтовий сценарій (XSS) програма приймає недовірені дані та надсилає їх у веб-браузер без належної перевірки.

Небезпечні прямі посилання на об’єкти (Insecure Direct Object References) розробник виставляє посилання на внутрішній об'єкт реалізації.

Помилка безпеки (Security Misconfiguration) Неправильне налаштування безпеки може надати зловмисникам несанкціонований доступ до системних даних або функцій.

Чутлива експозиція даних (Sensitive Data Exposure) Якщо веб-додатки не захищають конфіденційні дані належним чином за допомогою шифрування

Відсутній функціональний рівень контролю доступу (Missing Function Level Access Control) Якщо права доступу до рівня функцій не підтверджені,

Підробка міжміських запитів (CSRF, Cross-Site Request Forgery) відбувається, коли зловмисник змушує браузер користувача надсилати підроблені HTTP-запити, включаючи сесійні файли cookie.

Використання компонентів з відомими вразливими місцями (Using Components with Known Vulnerabilities) вразливі бібліотеки

Недійсні переадресації та пересилання (Unvalidated Redirects and Forwards) Веб-програми часто переспрямовують або пересилають користувачів на інші сторінки.

Управління додатками - це керування функціями введення, обробки та виведення. Вони включають методи, що допомагають забезпечити точність, повноту, валідність

Управління додатками включає: • Брандмауери • Програми шифрування • Програми проти зловмисного програмного забезпечення • Програми виявлення / видалення шпигунських програм • Біометрична автентифікація

Щоб знизити ризик безпеки додатків, OWASP рекомендує наступне: • Визначити вимоги безпеки програми • Використовувати належні практики архітектури безпеки додатків з самого початку розробки програми • Створити міцні та зручні засоби управління безпекою • Інтегрувати безпеку в життєвий цикл розробки • Будьте в курсі вразливості додатків

питання та витримки, пов’язані з бездротовим доступом:

1. Перехоплення чутливої інформації
2. Втрата або крадіжка пристроїв
3. Неправильне використання пристроїв
4. Відволікання, спричинене пристроями
5. Можливі наслідки використання пристрою для здоров'я
6. Бездротова аутентифікація користувачів
7. Захист файлів
8. Шифрування безпеки WEP
9. Сумісність
10. Точка перекладу

Вимоги до класифікації даних

При класифікації даних слід враховувати такі вимоги: • Доступ та автентифікація - визначте вимоги доступу, включаючи визначення профілів користувачів, критерії затвердження доступу та процедури перевірки. • Cекретність - визначте, де зберігаються чутливі дані та як вони передаються. • Конфіденційність - використовуйте елементи керування, щоб попередити постраждалого користувача про те, що його або її інформація буде використана. • Доступність - Визначте допуски на час роботи та простоя для різних типів даних. • Власність та розповсюдження - встановіть процедури захисту даних від несанкціонованого копіювання та розповсюдження. • Цілісність - захист даних від несанкціонованих змін за допомогою процедур контролю змін та автоматизованого моніторингу та виявлення від несанкціонованих змін та маніпуляцій. • Збереження даних - визначте періоди збереження та збережіть конкретні версії програмного забезпечення, обладнання, облікових даних для автентифікації та ключі шифрування, щоб забезпечити доступність. •Аудиторність - слідкуйте за доступом, авторизаціями, змінами та транзакціями. Після того, як буде призначена класифікація даних, можна встановити засоби безпеки, такі як шифрування, аутентифікація та реєстрація даних. Заходи безпеки повинні збільшуватися в міру збільшення рівня чутливості або критичності даних

1. Шкідливий програмний фрагмент, здатний до впровадження в інформаційну систему у тілі переданого користувачем файла в інші файли компʼютера, зокрема у файли системних і прикладних програм та електронної пошти.  
- Trojan horse  
2. Кібербезпека це:   
- Формування та здійснення процедур щодо захисту...  
3. Подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/ або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.  
- Incident  
4.Який зі стандартів відповідає за вимоги до організацій, що проводять аудит та сертифікацію систем управління інформаційною безпекою  
- ISO/IEC 27006:2007  
5. Типи шарів, необхідних для захисту в глибину (defense in depth):  
- Ізоляція, сегментація, внутрішній контроль та зовнішній контроль.  
6. Для побудови інформаційної безпеки компанії необхідно забезпечити таку функцію: придбання та супровід ліцензійного програмного та апаратного забезпечення, підписання продуктів використовуваних в компанії, розробка та обслуговування власних продуктів забезпечення захищеності всіх важливих інформаційних та комунікаційних процесів. Вкажіть як називається така служба:  
- Acquisition/ Development/ Maintenance  
7. Програма, яка використовує інтерфейсну карту мережі, що працює в нерозбірливому (promiscuous mode) режимі прийому і дозволяє перехоплювати всі пакети мережі.  
- Sniffer  
8. Яка з наведених нижче структур забезпечує виконання ролей кібербезпеки, які покладені на обовʼязок керувати інцидентами та обробляти їх  
- ﻿﻿Відділ(департамент) управління безпекою.  
9. Виберіть, що застосовується при використанні захисту периметру мережі(gecurity perimeter):  
- ﻿﻿Просканувати на виявлення мережевих портів для зловмисних дій.  
10. Документ, в якому зазначені правила користувачів про необхідні та заборонені дії та поведінку, називається:  
- Policies  
11. Вид кібератаки, який здійснює перенапрямлення жертви за помилковою (хибною) адресою:  
- pharming  
12. Актуальність і несуперечливість інформації, ті захищеність від руйнування та тесанкціонованого змінювання  
- цілісність  
13. Якщо було зафіксовано порушення кібербезпеки, то співробітники служби безпеки компанії (організації, установи) мають вжити таких заходів:  
- локалізувати область ІТ-інфраструктури, задіяної в інциденті.   
14. До основних загроз безпеки інформації відносяться:  
- компрометація інформації  
- розкриття конфіденційної інформації  
- відмова в обслуговуванні  
15. Рівень в OSI моделі, що забезпечує шифрування та стиснення даних, вибір форматів для передачі даних:  
- Presentation Layer  
  
**Test 2**1. Основними перевагами системи DMZ €:  
- Зловмисник повинен проникнути через три окремі пристрої  
- Внутрішні системи не мають прямого доступу до Інтернету  
- DMZ засновані на логічних, а не фізичних звʼязках  
Інтернету  
2. Схема Penetration Testing включає різні методи збору інформації, а саме:  
- ідентифікація операційних систем  
- ідентифікація служб  
- ідентифікація додатків  
3. Виберіть опис атаки Sniffer:  
- програма, яка використовує інтерфейсну карту мережі, що працює в нерозбірливому (promiscuous mode)

4. До функцій, доступних у IDS, належать:  
- Можливість збирання доказів про навʼязливу діяльн  
- Управління політикою безпеки  
5. SSL(Secure Sockets Layer) включає ряд основних етапів:  
- Симетричне шифрування трафіку на основі клююча  
- Відкритий ключ, обмін ключами на основі шифрування та автентифікація на основі сертифікатів  
- Однорангові узгодження для підтримки алгоритму  
  
**Test 3**

1. Виберіть з видів атак, які вказані:

спеціально сконструйовані коди, які за певною ознакою спричиняють деструктивну робот програми, що виконується, зокрема, повне припинення її виконання  
- Logic bOmbs  
2. Iнформаційна безпека корпорації включає  
- Security Management  
- Guidelines  
- Risk Management  
- Business Continuity/ Disaster Recovery  
- Firewall Management  
- Policies  
- Standards  
3. Поставте етапи фази проникнення в правильному порядку.  
1. Aтака  
2. Bикриття  
3. Звітність  
4. Планування  
4123  
4. До функцій, доступних у IDS, належать  
Управління політикою безпеки  
Виявлення вторгнень  
Можливість збирання доказів про навʼязливу діяльність  
5. У функції інформаційної безпеки корпораці (за ISACA) включас:  
побудова та відповідність операцій виконуваних в компанії згідно світових стай особливо стосовно інформаційної безпеки  
- Rules of Behavior  
- Acquisition/ Development/ Maintenance  
- Complance  
6. Виберіть правильно вказаний рівень для OSI моделі(формати, шифрування та стиснення даних)  
﻿﻿- Layer Presentation  
7. Фаза тестування SDLC включає:  
- Перевірку того, що програма, підсистема чи додаток та розроблені засоби безпеки виконують функці для яких вони були розроблені: інш компоненти системи  
- Різноманітні методики розробки та організаційні вимоги для забезпечення широкого спектру схем або рівнів тестування  
- Визначення того, чи працюють блоки, що випробовуються, без будь-яких несправностей або негативного впливу на інші компоненти системи  
8. Функції програми, повʼязані з ідентифікацією та аутентифікацією, часто реалізуються невірно, що дозволяє зловмисникам компрометувати паролі, ключі, токени, щоб ідентифікуватися користувачами системи.  
- Identification and Authentication Failures