Екзамен з відповідями

1. Три найбільш поширені елементи управління компанією, що використовуються для захисту інформації, є:
    - Шифрування, дозволи на доступ до файлів та контроль доступу.
    - Контроль доступу, ведення журналів та цифрових підписів.
    - Хеші, реєстрація та резервне копіювання.
    - **Резервування, резервне копіювання та контроль доступу.**
2. Вкажіть типи вразливостей веб додатків згідно класифікації (OWASP-10): посилання на зовнішні сутності в документах XML обробляються старими або погано налаштованими процесорами XML.
    - XSS (Cross Site Scripting)
    - Insecure Direct Object References
    - Injections
    - Missing Function Level Access Control
    - Broken Authentication and Session Management
    - Using Components with Known Vulnerabilities
    - Cross-Site Request Forgery, CSRF/XSRF
    - **XXE(Unvalidated Redirects and Forwards)**
    - Sensitive Data Exposure
    - Security Misconfiguration
3. Модель управління мережею Міжнародної організації зі стандартизації (ISO) визначає п'ять функціональних областей управління мережею (FCAPS). Виберіть, яка відповідає за: доступ до мережевих пристроїв та корпоративних ресурсів уповноваженим особам. Ця служба відповідає за автентифікації, авторизації, брандмауерах, сегментації мережі та сповіщеннях про спроби порушення безпеки.
    - **Управління безпекою(Security Management)**
    - Управління продуктивністю(Performance Management)
    - Управління конфігурацією(Configuration Management)
    - Управління обліком(Accounting Management)
    - Управління відмовами(Fault Management)
4. Інформаційна безпека корпорації включає:
    - **Risk Management**

- Guidelines
- **Communications and Operations**
- Firewall Management
- **Compliance**
- **Vendor Management**
- **Business Continuity/ Disaster Recovery**
- **Acquisition/ Development/ Maintenance**
- Security Management
- **Asset Management**
- **Rules of Behavior**
- Policies
- Standards

5. Поставте етапи тестування на проникнення в правильному порядку.
   a. Атака
   b. Викриття (discovery)
   c. Звітність
   d. Планування
   dbac
6. Основною перевагою системи DMZ є:
   - **Приватні мережеві адреси є закритими і не розголошуються**
   - **Внутрішні системи не мають прямого доступу до інтернету.**
   - DMZ засновані на логічних, а не фізичних зв'язках
   - **Зловмисник повинен проникнути через три окремі пристрої,**
   - Відмінна ефективність та масштабованість у міру зростання використання інтернету
7. **До функцій, доступних у IDS, належать:**
   - розкриття конфіденційної інформації
   - компрометація інформації
   - **збирання і документування даних про нав'язливу діяльність**
   - підготовка інфомації про управління політикою безпеки
   - отримання незаконної вигоди
   - **виявлення вторгнень**
8. Клас шкідливих програм, який приховує існування інших зловмисних програм шляхом зміни базової операційної системи.
   - Risk
   - Malware

- Standards
- Asset
- Threat
- Procedure
- **Rootkit**
- Patches
- Attack Vector
- Guidelines
- Identity Management
- Payload

9. Управління вразливістю в кібербезпеці починається з розуміння активів та їх розташування, що може бути досягнуто шляхом:
    - Сканування вразливості.
    - Матеріальне забезпечення
    - Переходу на ip-адреси
    - Тест на шкідливість.
    - Використання інструментів командного рядка.
    - **Ведення інвентаризації активів.**
10. Виберіть з видів атак, які вказані неправильно:
    - Phishing - використання зловмисником фальшивих e-mail та розсилка через соціальні мережі шахрайських повідомлень та різних типів вірусних програм з метою отримання доступу до конфіденційної інформації.
    - **Worm - різновид шкідливих програм, які маскуються під корисні додатки але наносять шкоду інформаційній системі: знищують або спотворюють інформацію на диску, викрадають паролі, спотворюють імена файлів і т.п.**
    - **Sniffer - атака з метою блокування ресурсів компютера або мережі компютерів через переповнення трафіку зовнішніми повідомленнями.**
    - **Exploit tools - шкідливий програмий фрагмент, здатний до впровадження в інформаційну систему у тілі переданого користувачем файла в інші файли комп'ютера, зокрема у файли системних і прикладних програм та електронної пошти.**
    - **Back door - вид атаки шляхом впровадження шкідливих команд або даних в працюючу систему з метою впливу на роботу так,**

щоб отримати доступ до комп'ютера чи даних, або дестабілізувати роботу системи загалом.

- IP-спуфінг (spoof) - вид хакерської атаки, що передбачає використання зловмисником, який видає себе за санкціонованого користувача, чужої IP-адреси.
- **Virus - злоякісна програма, яка забезпечує зловмиснику доступ до конфіденційної інформації на віддаленому комп'ютері.**
- Logic bombs - спеціально сконструйовані коди, які за певною ознакою спричиняють деструкт програми, що виконується, зокрема, повне припинення її виконання.
- DDoS-атака (Distributed Denial of Service) - скоординована атака відразу з багатьох комп'ютерів. Здійснюється шляхом провокування надмірного навантаження на ОС, додатки або технічні засоби мережі.
- **Trojan horse - злоякісні програми, здатні до самостійного створення своїх копій і розповсюдження їх по мережі**

11. Вкажіть рівень для OSI моделі, який перекладає мережеві адреси та маршрутизує дані від відправника до одержувача.
    - Layer Transport
    - Layer Program
    - **Layer Network**
    - Layer Application
    - Layer Presentation
    - Layer Physical
    - Layer Data Link
12. Фаза тестування SDLC включає:
    - Відкритий ключ, обмін ключами на основі шифрування та автентифікація на основі сертифікатів
    - Недоліки ін'єкції виникають, коли ненадійні дані надсилаються перекладачеві. Зловмисник може підманути перекладача виконувати ненавмисні команди або отримати доступ до несанкціонованих даних.
    - **Перевірку того, що програма, підсистема чи додаток та розроблені засоби безпеки виконують функції, для яких вони були розроблені; інші компоненти системи**
13. Спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-

комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем.

- **Attack**
- Policies
- Incident
- Threat

14. Яке з наведеного нижче є найкращим визначенням для кібербезпеки?
    - З**ахист інформаційних активів компанії шляхом адресації загроз інформації, обробки, зберігання або передачі взаємодіючими інформаційними системами**
    - Процес, за допомогою якого організація управляє ризиком кібербезпеки до прийнятного рівня
    - Захист паперових документів, цифрової та інтелектуальної власності та вербальних чи візуальних комунікацій
    - Захист інформації від несанкціонованого доступу чи розголошення