Схема локальної мережі KSE

1. Основні компоненти

- **Ключові комутатори**:
    - Комутатор 1
    - Комутатор 2
- **Мережеві маршрутизатори**:
    - Маршрутизатор 1
    - Маршрутизатор 2 (резервний)
- **Мережевий екран (Firewall)**:
    - Основний екран

2. Підключення

- **Вхід до мережі**:
    - Підключення до провайдера Інтернету (ISP).
- **Зв’язок між пристроями**:
    - Оптоволоконний зв’язок між ключовими комутаторами.
    - Ethernet-зв’язок між доступними комутаторами і кінцевими пристроями.

3. Сегментація мережі

- **Адміністративний сегмент**:
    - Сервери бухгалтерії, HR.
- **Студентський сегмент**:
    - Доступ до навчальних платформ.
- **Сегмент викладачів**:
    - Віддалений доступ до наукових ресурсів.
- **Гостьова мережа**:
    - Wi-Fi для відвідувачів (з обмеженим доступом).

4. Пристрої

- **Сервери**:
    - Файловий сервер.
    - Сервер автентифікації.
- **Кінцеві точки**:

    - Робочі станції.
    - Ноутбуки студентів.
    - Принтери.
- **Wi-Fi точки доступу**:
    - AP-1 (зона навчання).
    - AP-2 (зона адміністрації).

5. Логічна структура

- **Віртуальні локальні мережі (VLAN)**:
    - VLAN 10: Адміністрація.
    - VLAN 20: Студенти.
    - VLAN 30: Викладачі.
    - VLAN 40: Гості.
- **IP-підмережі**:
    - Адміністрація: 192.168.1.0/24.
    - Студенти: 192.168.2.0/24.
    - Викладачі: 192.168.3.0/24.
    - Гості: 192.168.4.0/24.

6. Додаткові сервіси

- **DNS-сервери**:
    - Внутрішній DNS для локальних доменів.
- **DHCP-сервери**:
    - Розподіл IP для студентської та гостьової мережі.
- **VPN**:
    - Для віддаленого доступу викладачів та адміністрації.

Темплейт для заповнення реальними девайсами.

Аналіз сценарію атаки на інфраструктуру Командно-штабного елементу (КШЕ) передбачає розгляд таких основних аспектів, як вектори атак, потенційні точки входу та методи захисту.

1. Карта мережі з потенційними точками входу

Командно-штабний елемент (КШЕ) зазвичай включає кілька компонентів: сервери, мережеві пристрої (маршрутизатори, комутатори), робочі станції та різноманітні пристрої для зв'язку. У мережі можуть бути як внутрішні (внутрішні сервери та робочі місця), так і зовнішні точки входу (мережі зв'язку, зовнішні служби доступу).

Потенційні точки входу:

1. **Інтернет-канали та з'єднання через VPN:**
    - Атакуючий може спробувати використати незащищені порти або експлойти в обладнанні, що з'єднує KSE з Інтернетом.
2. **Доступ через внутрішні облікові записи (під час атак на співробітників):**
    - Віруси, фішинг, чи інші методи соціальної інженерії можуть дати доступ до внутрішньої мережі КШЕ через слабкі паролі або зламані облікові записи.
3. **Вразливості в мережевих пристроях:**
    - Слабкі місця в налаштуваннях комутаторів, маршрутизаторів або брандмауерів можуть стати вразливими точками для атак через незащищені порти або відсутність останніх оновлень безпеки.
4. **Фізичний доступ до обладнання:**
    - Атаки через фізичний доступ до серверів чи робочих станцій співробітників можуть бути дуже ефективними, якщо захист фізичного доступу слабкий.
5. **Системи управління (SCADA, спеціалізовані термінали для збору та обробки даних):**
    - Атаки через вразливості в специфічному програмному забезпеченні для управління військовими чи стратегічними системами КШЕ.

2. Можливі вектори атак

1. **Фішинг та соціальна інженерія:**
    - Атакуючий може використовувати фішингові атаки для отримання доступу до внутрішніх облікових записів співробітників, що дасть йому доступ до систем КШЕ.
    - Використання зловмисних файлів у вкладеннях електронної пошти або на фальшивих вебсайтах для завантаження шкідливих програм.
2. **Атака через вразливості в ПЗ/ОС:**

- Використання відомих уразливостей в операційних системах або програмному забезпеченні, яке використовується в мережі КШЕ.
- Поширення вірусів або експлойтів, які дозволяють атакуючим отримувати несанкціонований доступ до мережі.

3. **DDoS-атака:**
   - Дистрибуція трафіку для перевантаження каналів зв'язку або мережевого обладнання, що призведе до тимчасової втрати доступу або до відмови в обслуговуванні (DoS).
4. **Атака на сервери управління (наприклад, через RCE - віддалене виконання команд):**
   - Використання вразливостей в серверному програмному забезпеченні (наприклад, Web-інтерфейсів адміністратора чи баз даних) для отримання доступу до критичних систем КШЕ.
5. **Проміжні атаки (Man-in-the-Middle, MITM):**
   - Перехоплення даних, що передаються по незашифрованих каналах зв'язку, або спроби змінити передану інформацію через внутрішню або зовнішню мережу.

3. Заходи щодо виявлення та запобігання атаці

1. **Використання сучасних методів шифрування:**
   - Забезпечення захищеного зв'язку через VPN з використанням сильних протоколів (AES, IPSec, OpenVPN тощо).
   - Шифрування всіх важливих каналів зв'язку, включаючи внутрішні мережі та резервні копії даних.
2. **Моніторинг та аналіз мережевого трафіку:**
   - Використання засобів IDS/IPS (системи виявлення/запобігання вторгненням) для постійного моніторингу трафіку та виявлення підозрілих активностей.
   - Регулярний аналіз логів з метою виявлення аномалій, таких як спроби доступу до заборонених ресурсів.
3. **Регулярні оновлення та патчінг:**
   - Постійне оновлення операційних систем, програмного забезпечення та мережевих пристроїв до останніх версій, що містять виправлення вразливостей.
   - Включення автоматичних оновлень, якщо це можливо.
4. **Контроль доступу та багатоетапна автентифікація (MFA):**

- Впровадження політики обмеження доступу на основі найменших привілеїв та використання багатофакторної автентифікації для доступу до критичних систем.
- Використання систем управління обліковими записами для моніторингу та контролю за активністю користувачів.

5. **Захист від DDoS-атак:**
   - Використання спеціалізованих рішень для захисту від DDoS-атак (наприклад, Cloudflare або аналогічні сервіси).
   - Моніторинг аномалій у мережевому трафіку для вчасного виявлення підозрілих атак.

4. План реагування на інцидент

1. **Оцінка інциденту:**
   - Визначення характеру атаки: аналіз симптомів (падіння доступу, зниження продуктивності, зміни в даних).
   - Ідентифікація точки входу та визначення масштабу атаки (локалізація уражених систем).
2. **Локалізація та обмеження збитків:**
   - Якщо атака триває, припинити доступ до заражених мереж або систем.
   - Перевести внутрішні сервери та критичні системи в офлайн, якщо це необхідно для запобігання подальшому поширенню.
3. **Пошук джерела атаки:**
   - Використовувати аналітичні інструменти для збору доказів (лог-файли, трафік, сліди на зламаних пристроях).
   - Визначити джерело атаки (IP-адреси, канали зв'язку) для подальшого реагування.
4. **Залучення експертів з кібербезпеки:**
   - Запросити зовнішніх консультантів з кібербезпеки (діджитальна форензика).
   - Провести спільну роботу з правоохоронними органами.
5. **Відновлення та посилення безпеки:**
   - Відновлення пошкоджених даних з резервних копій (переконатися, що резервні копії не заражені).
   - Оновлення програмного забезпечення та зміна паролів після атаки.
   - Перевірка систем на наявність залишкових вразливостей.

6. **Комунікація з керівництвом і сповіщення зацікавлених сторін:**
    - Інформувати керівництво, а також органи, що відповідають за безпеку національної інфраструктури (якщо атака може загрожувати національній безпеці).
    - Провести повідомлення клієнтів та партнерів, якщо атака має міжнародні наслідки.
7. **Післяінцидентний аналіз та покращення заходів безпеки:**
    - Аналіз результатів інциденту і вжиття заходів для посилення заходів безпеки.
    - Проведення тренувань з реагування на інциденти для персоналу.