Wnioski:

1. **Metasploit na Kali Linux:**

- W trakcie ataku sieciowego z użyciem Metasploita na Windows 10, uzyskano dostęp do systemu ofiary.
- Informacje uzyskane obejmują otwarte porty, dane o procesach oraz dostęp do systemu plików.
- Zagrożenia: Nieautoryzowany dostęp do systemu, możliwość kradzieży poufnych danych.
- Możliwości: Wykorzystanie zdobytych informacji do eskalacji uprawnień lub przeprowadzenia dalszych ataków.

2. **Delegacja Kerberos w ataku na Active Directory:**

- Atak polegający na przejęciu domeny Active Directory za pomocą delegacji Kerberos jest zaawansowaną techniką.
- Umożliwia atakującemu uzyskanie pełnej kontroli nad domeną.
- Zagrożenia: Pełna utrata kontroli nad środowiskiem Active Directory, możliwość wykonywania działań w imieniu innych użytkowników.
- Możliwości: Przeprowadzenie zaawansowanego ataku, dostęp do kluczowych zasobów w sieci.

3. **Analiza aktywnych i nasłuchujących portów:**

- Narzędzia takie jak Netstat i PowerShell pozwalają na identyfikację aktywnych i nasłuchujących portów.
- Uzyskane informacje obejmują stan połączeń, procesy odpowiedzialne za połączenia oraz stany portów.
- Zagrożenia: Wykrycie nieautoryzowanego ruchu sieciowego, identyfikacja potencjalnych luk w zabezpieczeniach.
- Możliwości: Skuteczne monitorowanie aktywności sieciowej, szybkie reagowanie na podejrzane połączenia.

4. **Konfiguracja serwera Windows 2019 i klienta Windows 10:**

- Konfiguracja karty sieciowej, ustawienia adresu IP, bramy, serwera DNS oraz instalacja usług IIS na kliencie.
- Dodatkowo, konfiguracja serwera z Windows 2019 z instalacją roli RDS, ustawieniem połączenia zdalnego, startem usługi SSH i tworzeniem reguł zaporowych.
- Zagrożenia: Niewłaściwa konfiguracja może prowadzić do luk w zabezpieczeniach, ułatwiając atakującym dostęp do systemów.

- Możliwości: Poprawna konfiguracja zwiększa bezpieczeństwo systemu, umożliwiając jednocześnie prawidłowe funkcjonowanie usług.

5. **Wnioski końcowe:**

- Skuteczna obrona przed atakami sieciowymi wymaga zrozumienia metod ataków i stosowania odpowiednich środków zabezpieczających.

- Monitoring aktywności sieciowej oraz regularna analiza otwartych portów są kluczowe dla szybkiego wykrywania potencjalnych zagrożeń.

- Prawidłowa konfiguracja serwerów i klientów, w tym zabezpieczenia, odgrywają kluczową rolę w utrzymaniu bezpieczeństwa w sieci.

- Edukacja i świadomość pracowników są istotne w prewencji przed zaawansowanymi atakami, a także w szybkim reagowaniu na ewentualne incydenty.