# Cybersecurity Incident Report

Pracujesz jako analityk ds. bezpieczeństwa w biurze podróży, które ogłasza wyprzedaże i promocje na firmowej stronie internetowej. Pracownicy firmy regularnie odwiedzają stronę internetową firmy, aby wyszukać pakiety wakacyjne, które mogą zainteresować ich klientów.

Pewnego popołudnia otrzymujesz automatyczne powiadomienie z systemu monitoringu, wskazujące na problem z serwerem WWW. Próbujesz odwiedzić witrynę firmy, ale w przeglądarce pojawia się komunikat o błędzie przekroczenia limitu czasu połączenia.

Używasz sniffera pakietów do przechwytywania pakietów danych przesyłanych do iz serwera WWW. Zauważasz dużą liczbę żądań TCP SYN pochodzących z nieznanego adresu IP. Serwer sieciowy wydaje się być przytłoczony natężeniem ruchu przychodzącego i traci zdolność odpowiadania na wyjątkowo dużą liczbę żądań SYN. Podejrzewasz, że serwer jest atakowany przez złośliwego aktora.

Tymczasowo przełączasz serwer w tryb offline, aby komputer mógł odzyskać i powrócić do normalnego stanu działania. Konfigurujesz również firmową zaporę ogniową, aby blokowała adres IP, który wysyłał nienormalną liczbę żądań SYN. Wiesz, że twoje rozwiązanie do blokowania adresów IP nie będzie działać długo, ponieważ osoba atakująca może sfałszować inne adresy IP, aby ominąć tę blokadę. Musisz szybko powiadomić swojego przełożonego o tym problemie i omówić kolejne kroki, aby powstrzymać atakującego i zapobiec ponownemu wystąpieniu tego problemu. Musisz być przygotowany na poinformowanie swojego szefa o typie wykrytego ataku i jego wpływie na serwer WWW i pracowników.

**W folderze znajdzie się logi z Wireshark oraz instrukcje odczytywania ich**

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| W czasie ataku dochodzi do wysłania ogromnych ilości pakietów SYN. Atak najprawdopodobniej pochodzi z pojedynczego adresu IP: 203.0.113.0 co sugeruje że doszło do typu ataku DoS - SYN flood attack |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Atak korzysta z działania TCP Three-way handshake gdzie po otrzymaniu pakietu SYN serwer odpowiada pakietem SYN,ACK i oczekuje na otrzymanie odpowiedzi zwrotnej ACK. Natomiast atakujący przesyła ciągle pakiety SYN ciągle inicjując TCP handshake. To powoduje przeciążenie mocy obliczeniowej serwera webowego i przez to zakłócenia w działaniu strony internetowej |