Analiza procesu 3-way handshake

Eksploatacja Lokalnych Sieci Komputerowych

Cele zajęć

1. Zaznajomienie się z procesem 3-way handshake w protokole TCP.
2. Śledzenie i analiza procesu nawiązywania połączenia w sieci przy użyciu Wiresharka.
3. Tworzenie raportu z analizy przechwyconego ruchu sieciowego.

Wprowadzenie

Protokół TCP (Transmission Control Protocol) jest niezawodnym protokołem warstwy transportowej, który zapewnia stabilne i kontrolowane połączenie między dwoma urządzeniami. Przed przesłaniem danych w połączeniu TCP, musi zostać nawiązane połączenie między nadawcą a odbiorcą. Proces ten nazywa się **three-way handshake** (lub **uzgadnianie trójetapowe**) i obejmuje trzy kroki:

1. **SYN** (Synchronize): Klient wysyła do serwera pakiet SYN, w którym informuje o chęci nawiązania połączenia.
2. **SYN-ACK** (Synchronize Acknowledgment): Serwer odpowiada pakietem SYN-ACK, potwierdzając odbiór i również prosząc o synchronizację.
3. **ACK** (Acknowledgment): Klient odpowiada pakietem ACK, potwierdzając nawiązanie połączenia.

Dopiero po tym trójfazowym procesie połączenie TCP zostaje nawiązane, a dane mogą być bezpiecznie przesyłane.

Śledzenie procesu 3-way handshake

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu sieciowego.
2. Zainicjuj dowolne połączenie TCP (np. otwórz stronę internetową w przeglądarce)
3. Zatrzymaj przechwytywanie ruchu po kilku sekundach, gdy połączenie TCP zostanie nawiązane.
4. Użyj filtra **tcp.flags.syn==1 && tcp.flags.ack==0** w Wiresharku, aby wyświetlić pakiety SYN wysyłane przez klienta.
5. Następnie filtruj **tcp.flags.syn==1 && tcp.flags.ack==1**, aby zobaczyć pakiet SYN-ACK wysłany przez serwer.
6. Na końcu użyj filtra **tcp.flags.ack==1 && tcp.flags.syn==0**, aby wyświetlić pakiet ACK potwierdzający połączenie przez klienta.

Analiza danych

1. Znajdź i oznacz w Wiresharku kolejne etapy procesu 3-way handshake (SYN, SYN-ACK, ACK).
2. Przeanalizuj zawartość każdego z pakietów, zwracając uwagę na pola, takie jak numer sekwencyjny (Sequence Number) i numer potwierdzenia (Acknowledgment Number).
3. Zrób zrzuty ekranu dla każdego z kroków i oznacz odpowiednie informacje (numery portów, adresy IP, sekwencje pakietów).
4. Wyjaśnij czym są numery sekwencyjne i numery potwierdzenia oraz dlaczego są istotne w transmisji TCP.

Śledzenie przerwanego połączenia (opcjonalnie)

1. Zainicjuj ponowne połączenie i spróbuj przerwać je, zanim zostanie w pełni nawiązane (np. rozłączając kabel sieciowy lub zamykając aplikację).
2. Przeanalizuj pakiety RST (reset), które zostaną wysłane, aby zakończyć próbę nawiązania połączenia.

Przygotuj krótki raport z przeprowadzonych działań. Umieść w nim wykonane zrzuty ekranu dla każdego etapu 3-way handshake (SYN, SYN-ACK, ACK). Oznacz w nich numery portów, adresy IP i numery sekwencyjne. Pracę zapisz jako plik .pdf i prześlij na adres szkola@davidkasperek.com