Badanie protokołów warstwy transportowej i aplikacji

Eksploatacja Lokalnych Sieci Komputerowych

Cele zajęć

1. Zaznajomienie się z protokołami warstwy transportowej (TCP i UDP) oraz aplikacyjnej (HTTP/HTTPS).
2. Analiza pakietów HTTP/HTTPS przy pomocy programu Wireshark.
3. Zapoznanie z protokołem SMTP oraz jego analiza.

Wprowadzenie

Warstwa transportowa w modelu OSI odpowiada za zarządzanie połączeniami między komputerami. Najważniejsze protokoły warstwy transportowej to TCP i UDP.

TCP (Transmission Control Protocol) – zapewnia niezawodne, uporządkowane przesyłanie danych.

UDP (User Datagram Protocol) – jest szybszy, ale mniej niezawodny, używany w sytuacjach, gdzie szybkość jest ważniejsza niż potwierdzenie dostarczenia danych.

Warstwa aplikacyjna odpowiada za bezpośrednią interakcję z użytkownikiem. Przykładami protokołów tej warstwy są HTTP i HTTPS, które służą do przesyłania stron WWW.

HTTP to protokół nieszyfrowany, natomiast **HTTPS** zapewnia bezpieczeństwo poprzez szyfrowanie danych za pomocą TLS.

Badanie protokołów warstwy transportowej

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu sieciowego.
2. Inicjuj różne połączenia, np. przeglądaj strony internetowe (ruch TCP) oraz uruchom aplikację korzystającą z UDP (np. streaming wideo, gry online).
3. Zatrzymaj przechwytywanie po kilku minutach.
4. Filtruj pakiety TCP (tcp) oraz UDP (udp).
5. Przeanalizuj kluczowe różnice między nagłówkami TCP i UDP: numer sekwencyjny, numer potwierdzenia (w TCP), brak mechanizmu potwierdzania w UDP.
6. Zrób zrzuty ekranu przedstawiające pakiety TCP i UDP oraz ich nagłówki.
7. Odpowiedz na poniższe pytania:
   - Czym różni się transmisja TCP od UDP?
   - Jakie są zalety i wady korzystania z TCP i UDP w różnych typach aplikacji?

Badanie protokołów warstwy aplikacji

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu sieciowego.
2. Otwórz przeglądarkę i odwiedź stronę korzystającą z HTTP (np. http://neverssl.com) oraz stronę HTTPS (np. https://www.google.com).
3. Zatrzymaj przechwytywanie.
4. Filtruj pakiety HTTP (http) oraz HTTPS (tls).
5. Przeanalizuj nagłówki HTTP, identyfikując kluczowe informacje takie jak metoda (GET/POST), User-Agent, Host, Content-Type.
6. Dla HTTPS, omów krótko znaczenie TLS i wyjaśnij, dlaczego ruch HTTPS jest zaszyfrowany.
7. Zrób zrzuty ekranu pakietów HTTP i TLS, omów różnice między nimi.

Badanie protokołu SMTP (opcjonalne)

SMTP (Simple Mail Transfer Protocol) to protokół warstwy aplikacji służący do przesyłania wiadomości e-mail między serwerami pocztowymi. SMTP działa na porcie 25 i wykorzystuje protokół TCP do niezawodnego przesyłania danych.

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu sieciowego
2. W wierszu poleceń (cmd/powershell) użyj narzędzia telnet lub nc (netcat) do nawiązania połączenia z serwerem SMTP: **telnet smtp.freesmtpservers.com 25**
3. Po nawiązaniu połączenia z serwerem, wpisz kolejne komendy SMTP, aby zasymulować wysyłanie wiadomości:
   - **HELO [twoja_domena]**
   - **MAIL FROM:<twojadres@example.com>**
   - **RCPT TO:<adresodbiorcy@example.com>**
   - **DATA**
   - Wprowadź treść wiadomości e-mail (np. „Test SMTP"), zakończ kropką (.) i naciśnij Enter.
   - **QUIT**
4. Zatrzymaj przechwytywanie ruchu w Wiresharku po zakończeniu sesji.
5. Użyj filtra smtp w Wiresharku, aby wyświetlić pakiety związane z przesyłaniem wiadomości SMTP.
6. Przeanalizuj pakiety, zwracając uwagę na komendy HELO, MAIL FROM, RCPT TO, DATA, i QUIT.
7. Zrób zrzut ekranu z przechwyconych pakietów SMTP, oznaczając istotne komendy i adresy nadawcy oraz odbiorcy.

Przygotuj krótki raport z przeprowadzonych działań. Umieść w nim wykonane zrzuty ekranu oraz odpowiedzi na pytania. Pracę zapisz jako plik .pdf i prześlij na adres szkola@davidkasperek.com