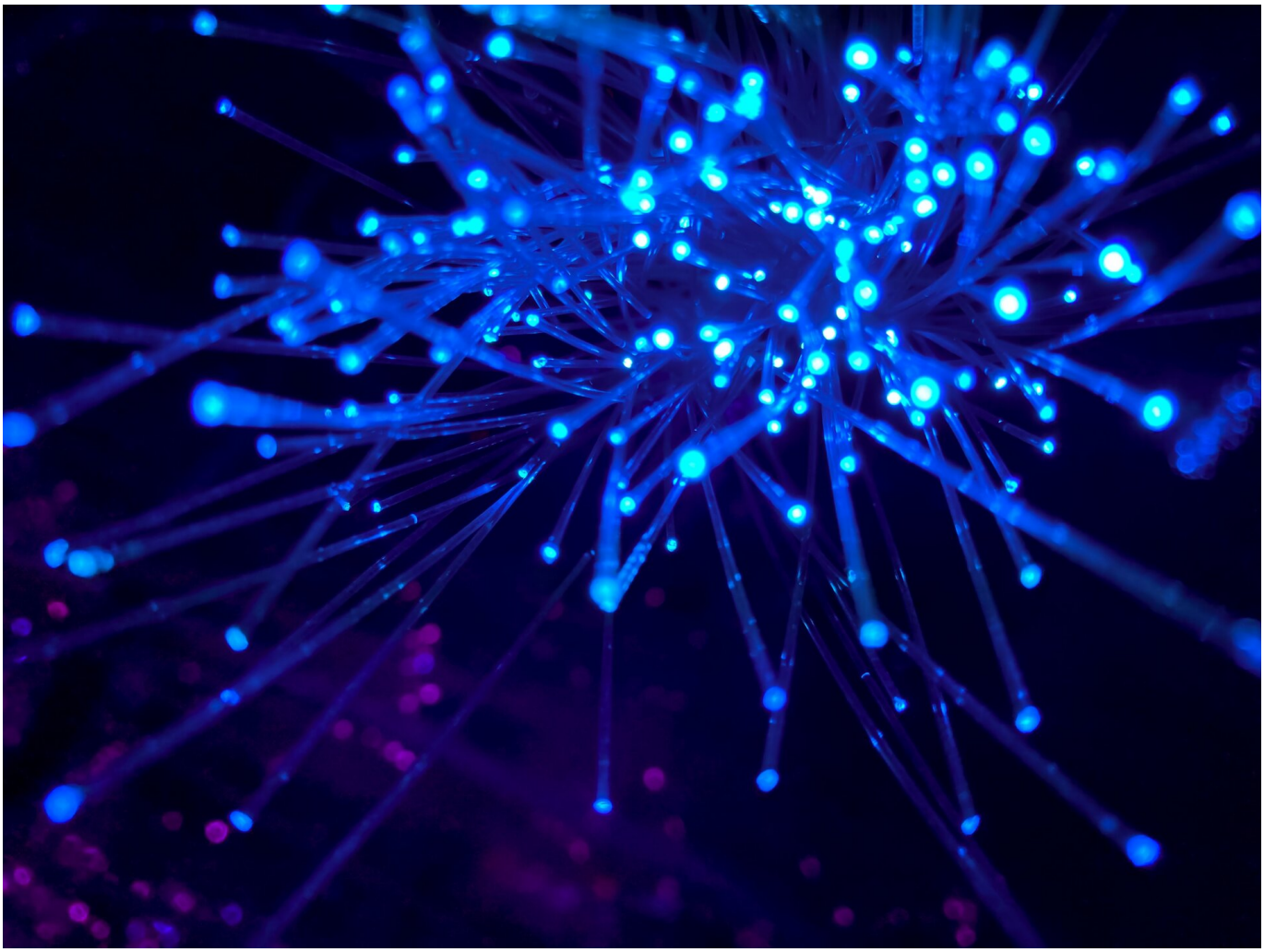


Śledzenie transmisji pakietów

Śledzenie transmisji pakietów

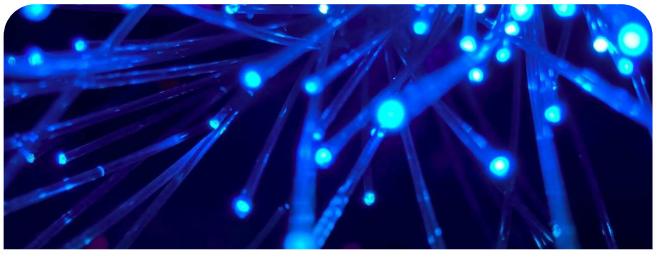
Źródło: JJ Ying, dostępny w internecie: unsplash.com, domena publiczna.

Komunikacja sieciowa to proces, na który składa się wiele elementów. Do tej pory rozważania na temat sieci komputerowych były oparte na teoretycznych modelach opisujących komunikacją sieciową. W tym e-materiale zajrzymy do karty sieciowej, przez którą przechodzą wszystkie dane przychodzące i wychodzące z naszego komputera. Przekonamy się, że te rozważania wcale nie były tylko teoretyczne.

Twoje cele

- Zapoznasz się z oprogramowaniem Wireshark do analizy pakietów sieciowych.
- Wyjaśnisz potrzebę stosowania szyfrowanej komunikacji.

Aby zrozumieć poruszane w tym materiale zagadnienia, przypomnij sobie:



Elementy aktywne i pasywne w sieci komputerowej

System nazw domen

Usługa SSH jako następca usługi Telnet

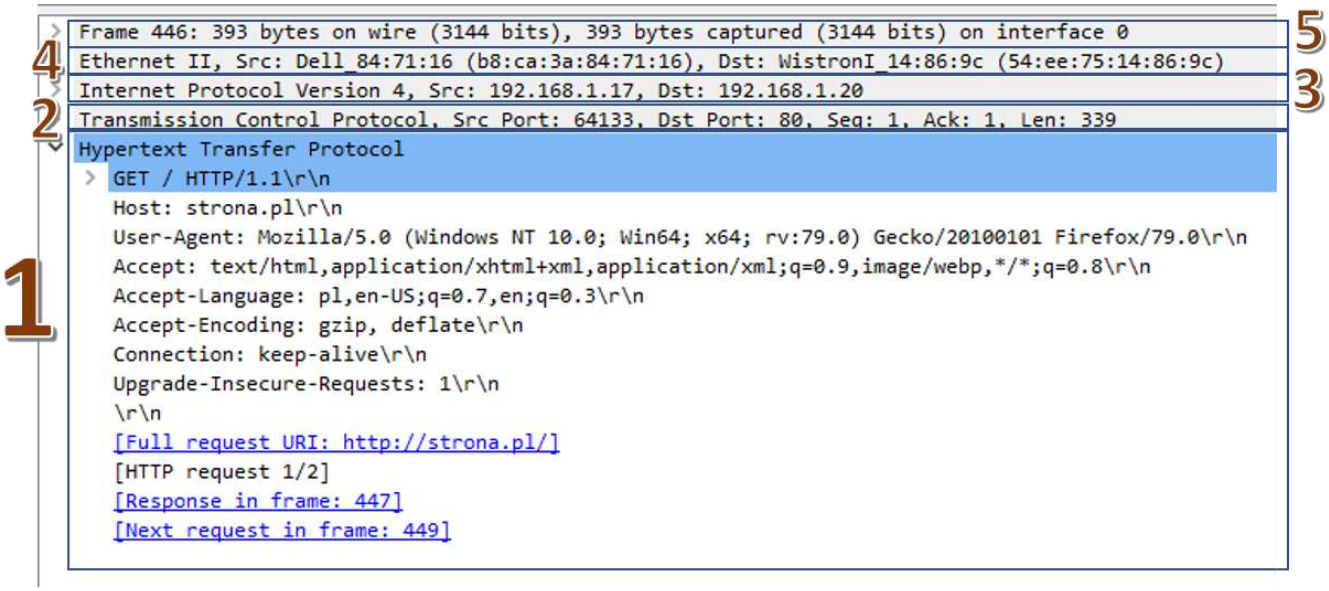
Poczta elektroniczna

Przeczytaj

Ruch sieciowy generowany podczas komunikacji między urządzeniami to zbiór pakietów przesyłanych między uczestnikami komunikacji sieciowej. Pakiety te da się przechwycić, by przeanalizować, co jest w nich przesyłane. Aby była możliwa taka analiza, niezbędne jest specjalne oprogramowanie typu **sniffer**. Jednym z najpopularniejszych programów tego typu jest **Wireshark**. Program jest darmowy i można go pobrać z oficjalnej strony projektu.

Enkapsulacja w praktyce

Poznaliśmy już wiele terminów związanych z sieciami komputerowymi. Jednym z takich terminów jest **enkapsulacja**, czyli przygotowanie danych w sposób opisany przez warstwowe modele do przesłania przez sieć.



Przykład enkapsulacji pakietu danych, dokładniej żądania GET strony WWW od serwera przechwycony przez program Wireshark

> **Ciekawostka**
>
> Warto zaznaczyć, że proces enkapsulacji w programie jest „odwrócony", to znaczy warstwa aplikacji jest na samym dole (punkt 1 grafiki), natomiast warstwa dostępu do sieci prawie na szczycie (punkt 4 grafiki). Z punktu widzenia analizy pakietów nie ma to żadnego znaczenia, warto jednak być tego świadomym.

1. **Warstwa aplikacji**, a dokładniej protokół HTTP przygotował żądanie GET strony WWW. Na grafice widać, że HTTP generuje nie tylko żądanie GET, lecz także dołącza do niego informacje o systemie operacyjnym klienta, numerze wersji przeglądarki oraz adres

domenowy. Warto zaznaczyć, że istnieje możliwość anonimizacji tych danych (blokowanie wysyłania takich informacji).
2. **Warstwa transportowa**, a dokładniej protokół **TCP** (ang. *Transmission Control Protocol*), przygotowała segment z danymi, które otrzymała od warstwy aplikacji (żądanie GET). Do segmentu dodała oczywiście numery portów aplikacji (port 80 dla serwera, ponieważ to usługa WWW, a dla klienta losowy numer, w tym przypadku to **64133**).

> **Ważne!**
>
> Nie tylko aplikacje serwera posiadają odpowiednie numery portów. Klient nawiązując połączenie z serwerem, również otwiera port komunikacyjny. Za każdym połączeniem numer portu jest wybierany losowo.

3. **Warstwa sieciowa (internetowa)**, a dokładniej protokół **IP** (ang. *Internet Protocol*) utworzyła pakiet danych i nadała mu adresu IP serwera i klienta.
4. **Warstwa dostępu do sieci**, a dokładniej protokół **Ethernet** utworzyła ramkę danych oraz nadała tej ramce adresy MAC kart sieciowych serwera i klienta.

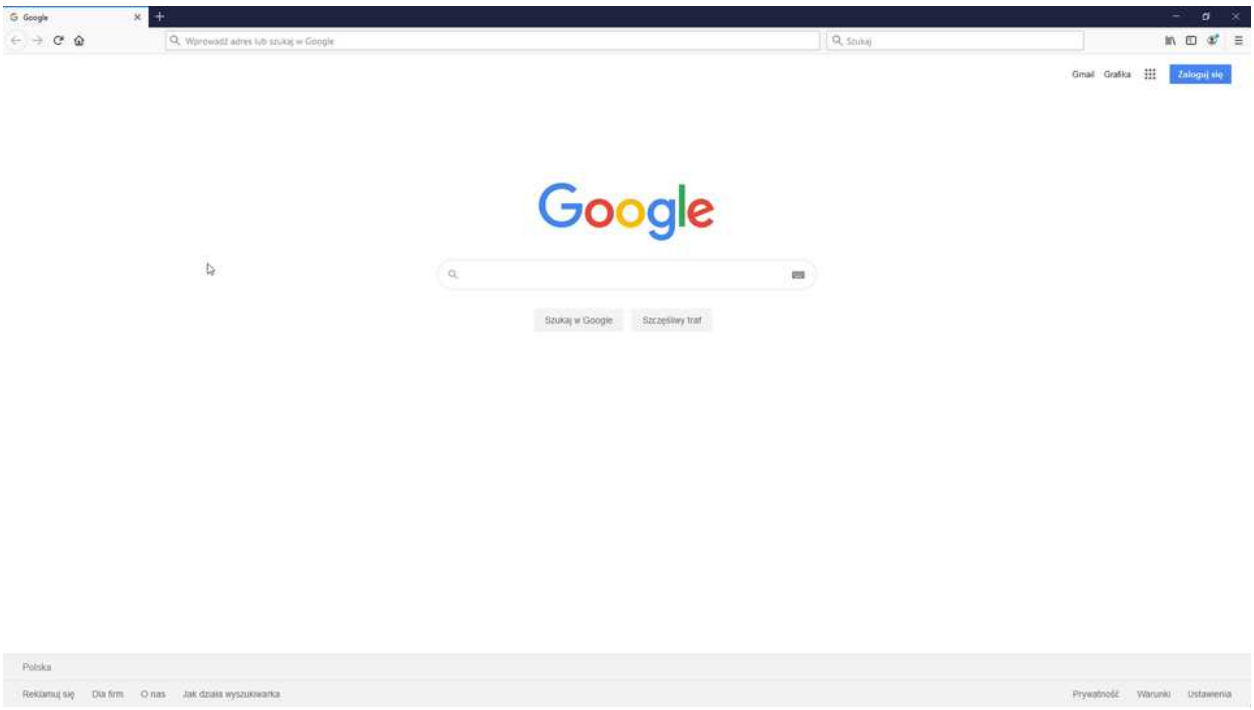
Na samym szczycie (punkt 5 grafiki) znajdują się informacje o numerze ramki, która została przesłana, a także o jej wielkości. Ramka przygotowana w ten sposób zostaje przesłana przez sieć.

Nie loguj się nigdzie tam, gdzie komunikacja nie jest szyfrowana

Obecnie zdecydowana większość witryn internetowych, a zwłaszcza tych, w których trzeba podawać swoje dane, takie jak chociażby **login** i **hasło**, stosuje protokół **HTTPS** zapewniający szyfrowaną komunikację między klientem a serwerem WWW. Niestety większość nie oznacza wszystkie, nadal więc możemy spotkać witryny, które, pomimo iż zapewnienie szyfrowania nie wymaga zbyt wiele wysiłku od administratora strony, takiej funkcji nie oferują. Być może administratorzy nie potrafią lub nie chcą tego zrobić, a to powinno dawać do myślenia. Unikajcie takich stron, ponieważ podane przez was dane prawdopodobnie trafią w niepowołane ręce. A bardzo łatwo odczytać chociażby login i hasło służące do logowania, jeśli dana strona nie szyfruje komunikacji, co przedstawiono poniżej:

Badanie 1

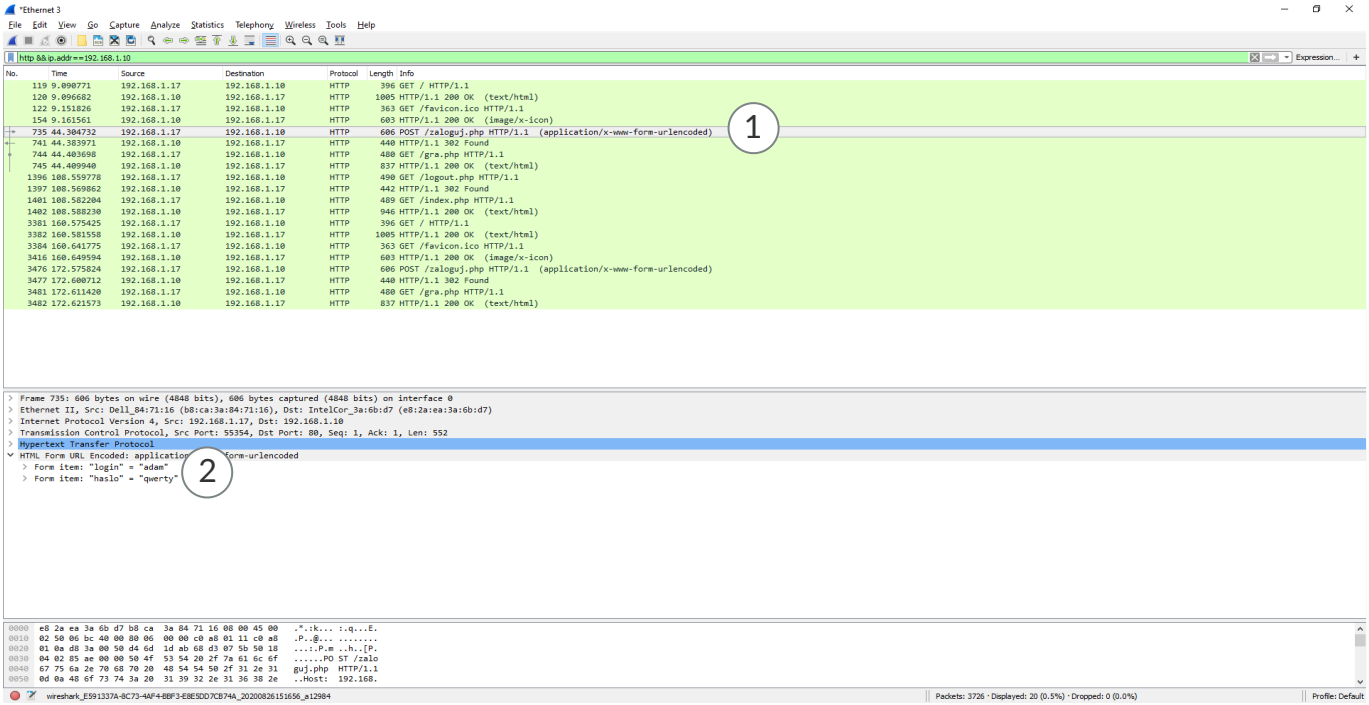
W przedstawionym wideo użytkownik wchodzi na przygotowaną stronę, która została umieszczona na serwerze WWW pracującym w sieci lokalnej (adresem strony jest adres IP tego serwera), i loguje się, podając login i hasło:



Film dostępny pod adresem /preview/resource/RCI6k9Jewzmqc

Film nawiązujący do treści materiału

W trakcie logowania działał w tle **Wireshark**. Zobaczmy, co przechwycił:



1

Metoda POST protokołu HTTP

Ten pakiet to element komunikacji HTTP przesyłający login i hasło do serwera WWW (metoda POST)

2

Zawartość komunikatu przesłanego metodą POST

Zawartość komunikatu POST przesłanego do serwera z widocznym loginem i hasłem

> **Ważne!**
>
> Zapamiętaj! Nie jesteś osobą anonimową w sieci! Każdy ruch sieciowy da się przechwycić i odczytać niektóre informacje. Bądź świadomym użytkownikiem sieci internet i pamiętaj, że nawet jeśli jest zaszyfrowana komunikacja między klientem a serwerem, to takie dane, jak np. adresy IP, są nadal przesyłane zazwyczaj bez szyfrowania, a to już pozwala namierzyć lokalizację osoby korzystającej z internetu.
>
> **Pamiętaj: nie hejtuj, nie obrażaj, nie dręcz. Współtwórz internet wolny od dyskryminacji i upokarzania kogokolwiek.**

Słownik

sniffer

rodzaj oprogramowania pozwalający śledzić komunikację sieciową

Animacja

Polecenie 1

Zapoznaj się z animacją i wykonaj ćwiczenie.

Film dostępny pod adresem /preview/resource/RumlV23hfZNko

Film nawiązujący do treści materiału

Ćwiczenie 1

Opracuj listę najważniejszych zasad, których powinno się przestrzegać, korzystając z sieci, jeśli nie chcemy, by ktoś przechwycił pakiety.

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Dokończ zdanie.

Aplikacje komputerowe pozwalające na przechwytywanie pakietów sieci komputerowej to...

- ◯ DDOSy.
- ◯ sniffery.
- ◯ man-in-the-middle.
- ◯ boty.

Ćwiczenie 2

Ułóż stos protokołów w odpowiedniej kolejności, na przykładzie komunikacji klienta z serwerem WWW.

- IP
- HTTP
- TCP
- Ethernet

Ćwiczenie 3

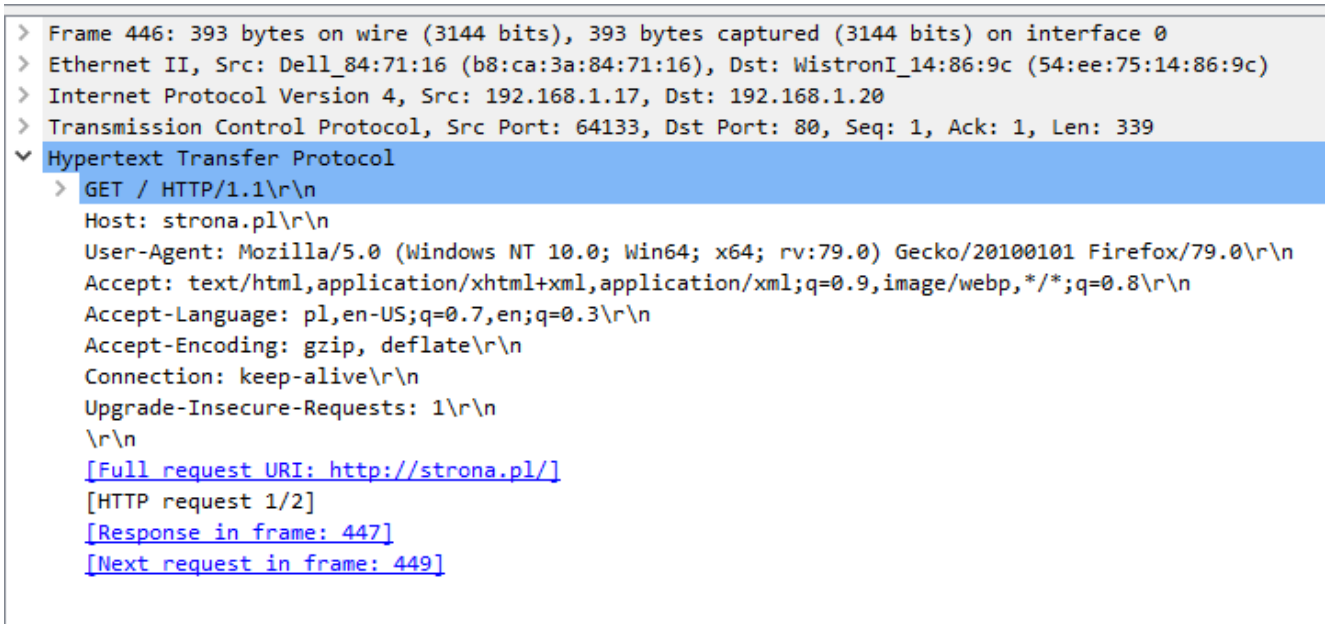
Wstaw w tekst odpowiednie słowa.

Programy typu [ ] pozwalają przechwytywać i [ ] komunikacje sieciową.

filtrować | rootkit | sniffer | analizować | zmieniać

Ćwiczenie 4

Wskaż, jaki numer portu aplikacji klienta widnieje na grafice z przechwyconego pakietu danych.



- ◯ 80
- ◯ 64134
- ◯ 192.168.1.17
- ◯ 64133

Ćwiczenie 5

Uzupełnij zdanie.

Warstwa dostępu do sieci, a dokładniej protokół [ ] utworzyła [ ] danych oraz nadała tej ramce adresy [ ] kart sieciowych serwera i klienta.

Ćwiczenie 6

Połącz w pary nazwy protokołów wraz z ich przykładowymi parametrami.

MAC/Ethernet	65843
TCP/UDP	64.69.234.6
IP	10-FE-ED-1B-43-8E

Ćwiczenie 7

Wstaw w zdanie odpowiednie słowa.

Warstwa [ ], a dokładniej protokół [ ], przygotowała segment z danymi, które otrzymała od warstwy aplikacji.

sieciowa | HTTP | IP | transportowa | TCP

Ćwiczenie 8

Wskaż, jakie informacje nie są przekazywane za pomocą żądania GET.

- ◯ akceptowany format danych
- ◯ silnik przeglądarki internetowej
- ◯ adres MAC klienta
- ◯ informacje o systemie operacyjnym klienta

Dla nauczyciela

Autor: Damian Stelmach
Przedmiot: Informatyka

Temat: Śledzenie transmisji pakietów

Grupa docelowa:

Liceum ogólnokształcące i technikum, liceum ogólnokształcące, technikum, zakres rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym: znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

Treści nauczania – wymagania szczegółowe

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi.

Zakres podstawowy. Uczeń:

4) charakteryzuje sieć internet, jej ogólną budowę i usługi, opisuje podstawowe topologie sieci komputerowej, przedstawia i porównuje zasady działania i funkcjonowania sieci komputerowej typu klient-serwer, peer-to-peer, opisuje sposoby identyfikowania komputerów w sieci.

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

3) opisuje warstwowy model sieci komputerowej oraz model sieci internet, opisuje podstawowe funkcje urządzeń i protokoły stosowane w przepływie informacji i w zarządzaniu siecią;

4) konfiguruje przykładową lokalną sieć komputerową oraz bezprzewodowy dostęp do sieci internet;

5) wyjaśnia, od czego zależy sprawne funkcjonowanie sieci komputerowej oraz szybki dostęp do jej usług i zasobów (parametry osprzętu sieciowego, szerokość pasma, zabezpieczenia typu ściana ogniowa i programy antywirusowe, możliwości serwera).

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Zapoznasz się z oprogramowaniem Wireshark do analizy pakietów sieciowych.
- Wyjaśnisz potrzebę stosowania szyfrowanej komunikacji.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Śledzenie transmisji pakietów". Nauczyciel prosi uczniów o zapoznanie się z multimedium w sekcji „Animacja".

Faza wstępna:

1. Nauczyciel wyświetla temat i cele zajęć. Prosi uczniów, by na podstawie wiadomości zdobytych przed lekcją zaproponowali kryteria sukcesu.Nauczyciel wyświetla i odczytuje temat lekcji oraz cele zajęć. Prosi uczniów o sformułowanie kryteriów sukcesu.

Faza realizacyjna:

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu zawartego w sekcji „Przeczytaj", jeśli nauczyciel - na podstawie raportu na platformie - uważa, że przygotowanie uczniów jest wystarczające, może pominąć tę czynność.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Animacja". Uczniowie wspólnie zapoznają się z animacją na temat analizy pakietów danych.
3. **Ćwiczenie umiejętności.** Uczniowie wykonują ćwiczenia nr 1-8 z sekcji „Sprawdź się". Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. Nauczyciel ponownie wyświetla na tablicy temat lekcji zawarty w sekcji „Wprowadzenie" i inicjuje krótką rozmowę na temat zrealizowanych celów (czego uczniowie się nauczyli).

Praca domowa:

1. Uczniowie wykonują ćwiczenie umieszczone pod animacją.

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj" można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.