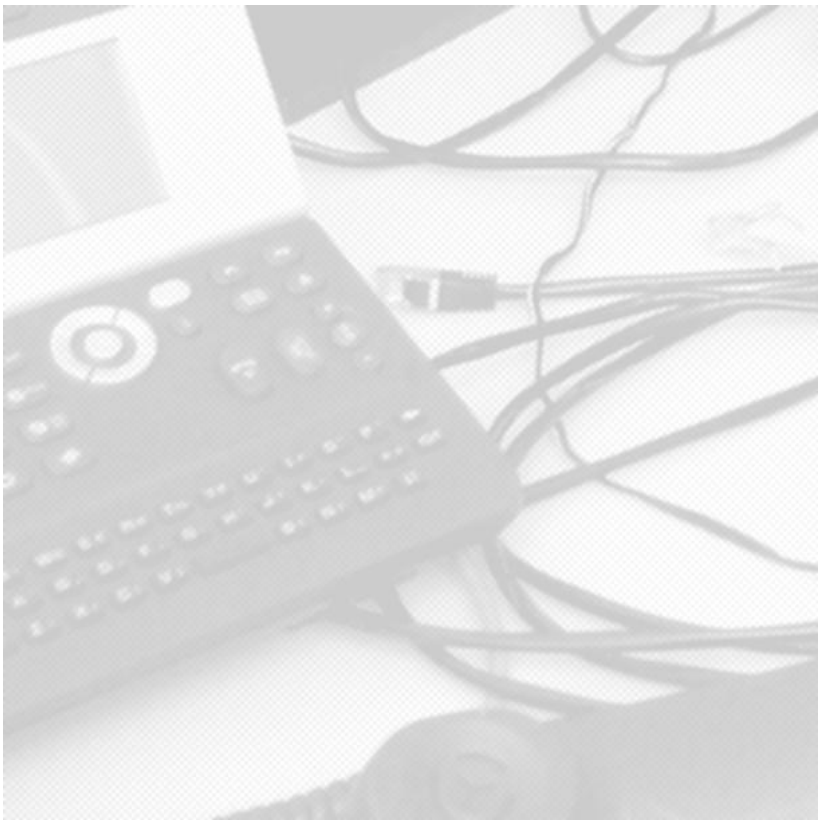
Zakład Cyberbezpieczeństwa
IT PW

LABORATORIUM SIECI

Instrukcja do ćwiczenia:
Warstwa fizyczna modelu TCP/IP oraz analiza ruchu sieciowego
Przedmiot: **Sieci Lokalne (LAN)**

Autor: Wojciech Mazurczyk
Aktualizacja: Artur Janicki



wersja 1.1
Warszawa, kwiecień 2015

ZCB - Zakład Cyberbezpieczeństwa
Instytut Telekomunikacji
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Część I: Warstwa fizyczna modelu TCP/IP

Cel: Zdobycie praktycznych umiejętności w wykonywaniu i testowaniu okablowania dla sieci LAN

Przebieg ćwiczenia:

a. Przedstawienie znanych rodzajów medium transmisyjnego oraz standardów okablowania UTP oraz ich zastosowania wykorzystywanych w sieciach LAN:
   a) straight-through
   b) crossover
   c) rollover

b. Przedstawienie sposobu działania i obsługi testera okablowania.

Zaliczenie: Każdy z uczestników laboratorium wykonuje jeden, wybrany rodzaj kabla oraz weryfikuje poprawność jego działania z wykorzystaniem testera kabli.

Część II: Przechwytywanie i analiza ruchu sieciowego

Cel: Zapoznanie się z możliwościami oraz obsługa snifferów na podstawie aplikacji **Wireshark**; analizowanie ruchu sieciowego na podstawie znanych protokołów

Przebieg ćwiczenia:

a. Prezentacja sposobu posługiwania się snifferem oraz analiza pozyskanych danych. Omówienie sposobu przedstawiania jednostek protokołów (PDU) w **Wireshark**.
b. Możliwości przedstawiania różnego rodzaju statystyk oraz wymiany wiadomości w sieci na poziomie różnych warstw modelu TCP/IP dla przechwyconego ruchu.

Zaliczenie: Stworzenie protokołu z laboratorium, w którym znajdzie się opis i rozwiązanie poniższych zadań do wykonania (proszę nie przepisywać pytań i odpowiadać zwięźle).

Zadania do wykonania:

1. Analiza stosu **TCP/IP** dla dowolnego, przechwyconego ruchu oraz nauka podstaw obsługi Wireshark.

2. Protokół **HTTP** - przechwytywać ruch sieciowy podczas logowania się na konto poczty internetowej – sprawdzić sposób zapisywania loginu i hasła dla protokołu HTTP.

   Znaleźć różnice w bezpieczeństwie logowania (z opcją „Bezpieczne logowanie" oraz bez):
   Portal Interia.pl (strona logowania od poczty: http://poczta.interia.pl):
   login: lablan10, hasło: lablan234

   Odpowiedz na pytania: jakie są sposoby przesyłania hasła w trakcie logowania do poczty z wykorzystaniem „czystego" protokołu HTTP oraz jaki protokół wykorzystywany jest do zabezpieczenia tej transmisji?

3. Protokół **HTTP** – sposób pobierania stron internetowych (wybrać adres dowolnej strony).

   Odpowiedz na pytanie: W jaki sposób następuje wymiana wiadomości protokołu HTTP pobranie elementów z wybranej strony WWW? (diagram wymiany wiadomości + krótki opis)

4. Protokół **FTP** – przechwycić ruch sieciowy podczas nawiązywania sesji protokołu FTP. Odnaleźć hasło w przesyłanym strumieniu.

   Odpowiedz na pytanie: W jaki sposób jest przesyłane hasło w protokole FTP?

   Adres serwera FTP: zostanie podany przez prowadzącego laboratorium
   User: lablan
   Password: lablan1
   Jako klienta FTP do połączenia do serwera FTP można wykorzystać dowolnie wybraną aplikację np. Eksplorator Windows lub klienta ftp uruchamianego z linii poleceń (ftp 192.168.14.x).

5. Protokół **TELNET** – ze skonfigurowanym wcześniej przez prowadzącego routerem zainicjować sesję telnet (prowadzący wpisuje hasło). Należy odnaleźć w przechwyconym strumieniu danych odnalezione hasło oraz sposób jego transmisji.

   Aby połączyć się przez sesję telnet z routerem należy użyć programy Putty, wybrać protokół *Telnet* i wpisać adres routera, podany przez prowadzącego.

   Odpowiedz na pytanie: W jaki sposób jest przesyłane hasło w protokole TELNET?

6. Protokół **ICMP** – analiza przechwyconego ruchu sieciowego po wydaniu komendy:
   `ping adres_IP`

   Odpowiedz na pytanie: Jakie wiadomości protokołu ICMP wykorzystywane są przez narzędzie ping?

7. Telefonia IP oparta na **SIP/RTP** – przechwycić i przeanalizować wiadomości sygnalizacyjne protokołu SIP oraz strumień głosowy pakietów RTP. Przechwycony ruch głosowy nagrać do pliku dźwiękowego.

   Konfiguracja klienta VoIP - 3CX Phone:
   1. Sprawdzić czy wybrany kodek to *G711* (Zakładka *Configuration* -> Przycisk *Codecs*).
   2. W polu *Username* wpisać wybraną nazwę użytkownika (Zakładka Configuration).
   3. Wyłączyć rejestrowanie się klienta VoIP do serwerów *proxy* i *registrar* (Zakładka *Configuration* -> checkbox *Proxy/registrar*).

   Aby zgrać przechwycony strumień RTP do pliku a następnie odtworzyć go w systemie Windows należy z włączonym **Wireshark** przechwycić rozmowę VoIP, następnie ją wyfiltrować (w pole filtr wpisać rtp) a następnie wybrać:
   Telephony -> RTP -> Stream Analysis -> Save Payload w formacie .au. Format .au jest odtwarzany np. przez Windows Media Player.

   Odpowiedz na pytanie: Narysuj przebieg wymiany wiadomości protokołu SIP od nawiązania połączenia do jego zakończenia (wskazówka: pomocna jest opcja *Telephony -> VoIP calls -> Flow* w menu programu Wireshark).

8. Sieci oparte na **hubach** vs. sieci oparte na **switchach**. Do wykonania tego zadania potrzebne jest połączenie trzech komputerów najpierw z wykorzystaniem huba a potem switcha. W każdym przypadku należy przechwytywać na jednej z maszyn ruch (a pomiędzy pozostałymi dwoma wygenerować jakiś ruch np. spingować jedną maszynę z drugiej).

   Uwaga: Wszystkie stacje robocze w laboratorium domyślnie są podpięte do tego samego switcha. Zatem przypadek sieci opartej na switchach można zrealizować na dowolonych 3 komputerach w laboratorium.

Do podłączenia 3 stacji roboczych poprzez hub należy pobrać hub od prowadzącego laboratorium.

Odpowiedz na pytania: Jaka jest podstawowa różnica pomiędzy przechwyconym ruchem przy podłączeniu przez hub oraz switch? Jak wytłumaczysz tę różnicę?

9. Analiza przechwyconego ruchu zapisanego w plikach **Wireshark**.

Odpowiedz na pytanie: Jakie sytuacje przedstawiają poszczególne pliki - jak zinterpretujesz takie wymiany wiadomości?