Grzegorz Wilczewski
ZST/IT/PW

Warszawa, 04/2015

OCHRONA INFORMACJI W SIECIACH (OINS)

ĆWICZENIE LABORATORYJNE #2

Analiza ruchu sieciowego

Informacje wstępne

Celem ćwiczenia laboratoryjnego jest analiza ruchu sieciowego w usłudze Voice over IP z wykorzystaniem analizatora Wireshark. Stworzone środowisko testowe jest wyizolowane i bazuje na rozwiązaniu marki 3CX. Poniższe zadania służą jedynie ukazaniu niektórych zagadnień związanych z aspektami ochrony informacji w sieciach telekomunikacyjnych. Należy pamiętać, że nieautoryzowany dostęp, nagrywanie i przetwarzanie rozmów telefonicznych przez osoby nieuprawnione jest naruszeniem tajemnicy korespondencji (Art. 267 K.K.).

Przebieg ćwiczenia

Ćwiczenie laboratoryjne #2 składa się z 4 etapów:

- W pierwszym kroku należy określić podstawowe parametry aktywnego połączenia sieciowego (bazowa adresacja).
- W drugim etapie poddaje się analizie proces rejestracji użytkownika końcowego w usłudze VoIP 3CX (analiza mechanizmów protokołu SIP).
- Kolejny krok to proces nawiązania połączenia z wybranym klientem (użytkownicy zestawiają połączenia według danych zawartych w tabeli Tab. 1.); w celu poprawnego przebiegu zadania maksymalnie 5 hostów może inicjalizować połączenie.
- W ostatnim etapie należy zanalizować dane multimedialne nawiązanego połączenia (rodzaj użytych protokołów, koderów mediów, parametrów sesji).

Tab. 1. Macierz zestawianych połączeń

Extension #	106	107	108	109	110
101	•				
102			•		
103		•			
104				•	
105					•

Zadania

Realizacja ćwiczenia laboratoryjnego wymaga wykonania następujących poleceń, według podanej kolejności:

1. **Inicjalizacja**:
   - uruchomić linię komend poleceniem z powłoki: `cmd`,
   - odczytać konfigurację aktywnego adaptera sieciowego (np. polecenie `ipconfig`); wynotować w raporcie następujące dane: `Adres IP`, `Maska podsieci`, `Brama domyślna`.

2. **Zagadnienie 1**. Rejestracja użytkownika w serwerze SIP:
   - uruchomić narzędzie `Wireshark`; w głównym oknie programu zlokalizować sekcję `Capture` – służącą do wyboru adaptera sieciowego do przechwytywanie ruchu, z listy `Interface List` wybrać urządzenie zgodne z `Nazwą kontrolera` z punktu *Inicjalizacja* z ćwiczenia #1.

- w oknie programu `Wireshark` z listy `Capture` wybrać polecenie `Start`; uruchomić aplikację 3CXPhone (klient VoIP); przechwycić wygenerowany ruch sieciowy w programie `Wireshark`, zakończyć przechwytywanie poleceniem `Stop` z listy `Capture`;
- udzielić odpowiedzi na następujące pytania:
  - jakie kryterium filtrowania należy zastosować by zaobserwować unikalne pakiety (podaj nazwę i wersję protokołu, określ typ: sygnalizacyjny / transportowy),
  - jaki jest adres serwera VoIP oraz port wybrany do świadczenia usługi,
  - ile i jakie wiadomości zostają przesłane pomiędzy klientem a serwerem,
  - jakie 2 kluczowe metody protokołu SIP zostały użyte w tym scenariuszu,
  - analizując odpowiedni (inicjalizujący) pakiet klienta podaj: nazwę użytkownika, adres VoIP w formacie SIP-URL, rodzaj użytego oprogramowania, dozwolone metody protokołu SIP,
  - analizując odpowiedni (odpowiedź na polecenie REGISTER) pakiet serwera podaj: rodzaj wiadomości / odpowiedzi SIP, wyszukaj informacje dotyczące szyfrowania (czy jest obecnie wymagane, jaki rodzaj jest preferowany).

3. **Zagadnienie 2.** Nawiązanie połączenia:
   - w oknie programu `Wireshark` z listy `Capture` wybrać polecenie `Start` (jeżeli pojawi się zapytanie, zanegować zapisywanie aktualnego zrzutu pakietów); w uruchomionej aplikacji 3CXPhone wybrać odpowiedni numer docelowy adresata, potwierdzić chęć nawiązania połączenia (symbol słuchawki na zielonym tle), **wybrany adresat zobligowany jest do zaakceptowania nadchodzącego połączenia**; przeprowadzić przynajmniej 30 sekundową rozmowę z wybranym adresatem; przechwycić wygenerowany ruch sieciowy w programie `Wireshark`, zakończyć przechwytywanie poleceniem `Stop` z listy `Capture`; w aplikacji 3CXPhone rozłączyć nawiązane połączenie.
   - udzielić odpowiedzi na następujące zagadnienia:
     - jaka wiadomość SIP rozpoczyna nawiązywanie połączenia,
     - podaj nazwę protokołu, który reprezentuje wiadomość załączona do pakietu inicjalizującego połączenie, podaj długość tej wiadomości oraz jej rodzaj,
     - z ilu etapów składa się proces nawiązania połączenia pomiędzy klientami,
     - ile wiadomości służy przeprowadzeniu autentykacji stron.

4. **Zagadnienie 3.** Analiza danych multimedialnych nawiązanego połączenia:
   - z przechwyconej sesji połączenia głosowego, w narzędziu `Wireshark`, w głównym oknie programu zlokalizować pakiet potwierdzający wynegocjowane zestawienie połączenia; zanalizować przeniesiony *payload SDP* udzielając odpowiedzi na następujące zagadnienia:
     - jaki rodzaj sesji multimedialnej został zestawiony (wskazówka: pole [s]),
     - podaj porty, na których należy oczekiwać ruchu danych audio oraz video,
     - jaki rodzaj protokołu jest użyty do przenoszenia danych multimedialnych w zestawionej sesji VoIP,
     - podaj preferowane kodery audio, częstotliwość próbkowania ścieżki audio.
   - w oknie programu `Wireshark` zmienić kryterium filtrowania zebranych pakietów na parametr `rtp.payload` ; porównać rodzaj kodeka audio z pakietów RTP z danymi z pakietu SDP; w oknie programu `Wireshark` wybrać polecenie `Telephony -> VoIP Calls` ; w nowym oknie zidentyfikować połączenie głosowe; wybrać polecenie `Player -> Decode` ; zaznaczyć odpowiedni strumień i wcisnąć polecenie `Play` ; odsłuchać przechwycone strumienie audio.
   - zadanie dodatkowe: próba identyfikacji kodera danych na podstawie rozmiaru pakietów.