Grzegorz Wilczewski
ZST/IT/PW
Warszawa, 04/2015

OCHRONA INFORMACJI W SIECIACH (OINS)

ĆWICZENIE LABORATORYJNE #1

Analiza ruchu sieciowego

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`, komunikat pomocy uzyskujemy parametryzując komendę przełącznikiem `-h`); wynotować w raporcie następujące dane: `Nazwa kontrolera (OPIS), Adres fizyczny, Adres IP hosta, Maska podsieci, Brama domyślna.`

2. **Zagadnienie 1**. Analiza ruchu sieciowego podstawowymi narzędziami systemowymi:
   - w nowej powłoce linii komend (`cmd`) wpisać polecenie: `ping -h`, wynotować w raporcie do czego służy komenda `ping`; podać znaczenie parametrów: `-i, -n, -t`; udzielić odpowiedzi na następujące pytania:
     - czym różni się rezultat wykonania polecenia `ping [Adres IP hosta]` od `ping [Adres IP hosta] –n 4`
     - w jaki sposób można przerwać ciągłe odpytywanie hosta w poleceniu `ping -t`
     - jaka minimalna wartość (graniczna) parametru `–i` pozwala na odpytanie hosta `wp.pl` , spróbuj określić ilość węzłów będących na drodze pakietu.

     Sprawdzić i wynotować rezultaty polecenia `ping wp.pl`, podać statystykę ruchu (pakiety, czas odpowiedzi) oraz adres hosta po przetłumaczeniu na format IP.
   - w nowej powłoce linii komend wpisać polecenie: `tracert -?` ; opisać znaczenie komendy `tracert`; określić znaczenie przełączników: `-d, -h` ; wykonać i zanalizować rezultaty polecenia `tracert wp.pl` (podać liczbę przeskoków oraz liczbę urządzeń pomiędzy hostem *testującym* a *testowanym*); porównać otrzymany wynik z liczbą węzłów określoną w metodzie `ping`; uruchomić polecenie z przełącznikiem `–d`, wyznaczyć najdłuższy czas odpowiedzi oraz wynotować adresy IP wszystkich węzłów na trasie.
   - w nowej powłoce linii komend wpisać polecenie: `netstat –h` ; podać znaczenie funkcji `netstat`; określić znaczenie przełączników: `-e, -p, -s` ; określić statystykę TCP oraz UDP stanu aktualnego (wynotować wartości *Odebrane/Wysłane*); uruchomić przeglądarkę, wpisać i wykonać dostęp do adresu: `http://citcom.tele.pw.edu.pl`, ponownie sprawdzić statystykę TCP/UDP, określić przyrost segmentów/datagramów.

3. **Zagadnienie 2.** Analiza ruchu sieciowego z wykorzystaniem narzędzia `NMAP`:
   - uruchomić narzędzie `Zenmap` (graficzna nakładka na `NMAP`); znaczenie wybranych pól: `Cel` – adres bądź pula adresów do zmapowania, `Profil` – zakres i technika procesu skanowania, `Komenda` – umożliwia dokładne sparametryzowanie kampanii mapowania, `Skan` – przycisk wyzwalający procedurę z pola `Komenda`.
   - przeliczyć `maskę podsieci` z punktu *Inicjalizacja*, na notację CIDR (zapis dziesiętny), wynotować wartość w raporcie.

- uruchomić skanowanie portów gdzie `Cel` to [`brama domyślna`]/[`maska podsieci CIDR`], `Profil` [`Regular scan`], `Komenda` rozszerzona o parametr `--top-ports 10`. Zakończenie procesu skanowania zostanie potwierdzone linią: `NMAP done:` w zakładce `Wyniki działania Nmapa`. Wynotować czas skanowania, liczbę przeskanowanych adresów oraz ilość aktywnych hostów.
- Po zakończeniu mapowania wykonać następującą analizę:
  - przesortować wyniki skanowania z listy `Hosty` według rosnącego kryterium w kolumnie `Host`. Wypisać pierwszy i ostatni aktywny adres IP. Wynotować całkowitą liczbę wyszczególnionych hostów.
  - z analizowanej listy wybrać hosta o adresie IP zgodnym z adresem `brama domyślna`, przełączyć aktywne okno na zakładkę `Porty / Hosty`. Sporządzić tabelę zawierającą listę przeskanowanych portów, wykorzystywany protokół, stan portu oraz usługę, która jest do niego przypisana. Podać znaczenie i zastosowanie portów `21, 22, 80, 110, 443`.
  - przełączyć aktywne okno na zakładkę `Topologia`, włączyć opcje `Promienie` oraz `Sterowanie`, z obszaru grafu topologii wybrać hosta reprezentującego maszynę lokalną (domyślnie funkcja `Change Focus` w zakładce `Akcja`, adres IP hosta z punktu *Inicjalizacja*); w przypadku wizualnie nieczytelnej topologii dopasować opcje sekcji `Widok`: odznaczyć pozycję `hostname`, wyregulować `Przybliżenie`, `Odstęp pierścieni` oraz pozycję `Zmniejsz odstęp pierścieni`, opcjonalnie zmienić `Promień koła`, `stopień natężenia` oraz `stopień rozprzestrzenienia` grafu topologii. Zamieścić w raporcie aktualną topologię sieci.

4. **Zagadnienie 3.** Analiza ruchu sieciowego z wykorzystaniem analizatora `Wireshark`:
   - 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*.
   - w oknie programu `Wireshark` z listy `Capture` wybrać polecenie `Start`; w nowej powłoce linii komend (`cmd`) wpisać polecenie: `ping [brama domyślna]`, przechwycić rezultaty uruchomionej komendy w programie `Wireshark`, zakończyć przechwytywanie poleceniem `Stop` z listy `Capture`; jaki protokół jest używany do realizacji polecenia ping, jakie wiadomości zostają przesłane?
   - uruchomić przeglądarkę, w oknie programu `Wireshark` z listy `Capture` wybrać polecenie `Start` (jeżeli pojawi się zapytanie, zanegować zapisywanie aktualnego zrzutu pakietów), w oknie przeglądarki wpisać i wykonać dostęp do adresu: `http://www.tiz.tele.pw.edu.pl`, zakończyć przechwytywanie poleceniem `Stop` z listy `Capture`; jakie kryterium filtrowania należy zastosować by zaobserwować transakcje dostępu do podanej strony (wskazówka: wykorzystany protokół), z iloma hostami nawiązano połączenie, jakie polecenie inicjuje dostęp do adresu strony, jaki standard protokołu został użyty, jakie informacje znajdują się w polu `User-agent` w pakiecie inicjującym dostęp do adresu, jaka wiadomość oznajmia zakończenie procesu pobierania strony?