Instrukcja 9 - Analiza ruchu ICMP, ARP i DNS

9.1 Cel ćwiczenia

W ćwiczeniu tym należy **powtórzyć** zadania opisane w laboratoriach 5 i 6, przechwytując i analizując szczegółowo (program Wireshark) powstały **ruch** sieciowy - związany z protokołami ICMP, ARP i DNS.

9.2 Instrukcje z laboratorium 5 (PSK-5)

9.2.1 Zadanie 1

Korzystając z programu **ping** należy sprawdzić dostępność serwerów znajdujących się w różnych lokalizacjach, np.:

- Instytut Inteligentnych Systemów Informatycznych,
- Wydział Inżynierii Mechanicznej i Informatyki,
- Strona główna politechniki Częstochowska,
- Częstochowa, poza Politechniką Częstochowską,
- Instytucje w Polsce, poza Częstochową,
- Instytucje w Europie poza Polską,
- ...

9.2.2 Zadanie 2

Korzystając z przełączników programu **ping** zbadać maksymalną wielkość ramki przekazywanej przez routery pośredniczące.

9.2.3 Zadanie 3

Korzystając z programu **tracert** należy uzyskać listę routerów pośredniczących w komunikacji z serwerami z Zadania 1. Zinterpretować różnorodność postaci uzyskanych wyników dla poszczególnych routerów.

9.2.4 Zadanie 4

Zasymulować działanie programu **tracert** za pomocą wielokrotnego wywołania programu **ping** (dla wszystkich serwerów z listy routerów pośredniczących) dla dowolnego serwera z Zadania 1.
Uwaga: to i inne "wyszarzone" zadania można pominąć.

9.2.5 Zadanie 5

Wykorzystując narzędzie **Monitis Visual Trace Route Tool** znaleźć serwer o jak największej liczbie zaznaczonych na mapie przeskoków. Czy pokonywana droga jest optymalna? **Uwaga:** w tym zadaniu wystarczy przejrzeć ruch sieciowy dla protokołu **http** od czasu uruchomienia testu na stronie.

9.3 Instrukcje z laboratorium 6 (PSK-6)

1. Wyświetlić pełne informacje o kartach sieciowych i połączeniach *ipconfig -all*.

2. Za pomocą polecenia **ipconfig** wyświetlić wszystkie serwery dns, zwolnić wszystkie adresy IP, ponownie wyświetlić wszystkie serwery dns, odnowić wszystkie adresy IP.

3. Przeglądając serwery dns *ipconfig /displaydns* **wyszukać kilka wpisów** o typie rekordu różnym od A (Host) i AAAA (np. CNAME, PTR). W celu szybszego wyszukiwania wyniki polecenia można zapisać do pliku lub zastosować wyszukiwanie: *ipconfig /displaydns | findstr /r /c:"Record[.]*:"*
W przypadku braku wpisów należy odwiedzić kilka różnych witryn internetowych.

4. Za pomocą polecenia **arp** wyświetlić wszystkie wpisy adresów w trybie pełnym. Następnie stosując podając odpowienie **adresy** - *inet_addr* oraz *-N if_addr* wyświetlić tylko wybrane przez nas wpisy.

5. Za pomocą polecenia arp **spróbować** dodać i usunąć wpisy z tablicy wpisów.

6. Za pomocą polecenia **nslookup** pobrać adres IPv4 (type=A), IPv6 (type=AAAA) oraz nazwy serwerów dns (type=NS) dla kilku wybranych domen (m.in. pcz.pl, google.pl itp).

7. Za pomocą polecenia **nslookup** zmienić serwer domyślny na 1 z serwerów DNS uzyskany w ćwiczeniu 6. Spróbować pobrać dane na temat wybranych **przez siebie** domen.

8. Uruchomić ponownie nslookup, zmieniając typ rekordów DNS na: CNAME, MX, PTR, SOA, SRV spróbować pobrać informacje dla kilku wybranych domen (m.in. **www**.pcz.pl, google.pl, itp)

9.4 Sprawozdanie

Studenci pracują i przygotowują sprawozdania w parach. W sprawozdaniu należy przedstawić przebieg przeprowadzonych eksperymentów (wygenerowany podczas wykonywania poleceń ruch sieciowy).