LABORATORIUM PROJEKTOWANIE I OBSŁUGA SIECI KOMPUTEROWYCH II

Data wykonania ćwiczenia:	09.04.2023
Rok studiów:	3
Semestr:	6
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	6

Temat: Eksploracja ruchu DNS / Demonstracja działania listy ACL

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Wireshark - Eksploracja ruchu DNS

Krok 1: Przechwytywanie ruchu DNS.

Otwórz Wireshark i rozpocznij przechwytywanie Wireshark, klikając dwukrotnie interfejs sieciowy z ruchem.

W wierszu polecenia wprowadź `ipconfig /flushdns` i wyczyść pamięć podręczną DNS

```
> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

W wierszu polecenia wprowadź polecenie `nslookup`, aby przejść do interaktywnego trybu nslookup.

Wprowadź nazwę domeny. W tym przykładzie używana jest nazwa domeny www.cisco.com. Wprowadź www.cisco.com za znakiem zachęty >.

```
> nslookup
Default Server:  UnKnown
Address:  68.105.28.16

> www.cisco.com
Server:  UnKnown
Address:  68.105.28.16

Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2001:578:28:68d::b33
          2001:578:28:685::b33
          96.7.79.147
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

Po zakończeniu wpisz exit, aby wyjść z interaktywnego trybu nslookup. Zamknij okno linii komend.

Kliknij przycisk Zatrzymaj przechwytywanie pakietów , aby zatrzymać przechwytywanie Wireshark

Krok 2: Przeglądanie zapytań DNS

Obserwuj ruch przechwycony w okienku Lista pakietów Wireshark. Wprowadź udp.port == 53 w polu filtru i kliknij strzałkę (lub naciśnij klawisz Enter), aby wyświetlić tylko pakiety DNS.

Wybierz pakiet DNS z etykietą Standardowa kwerenda 0x0002 A www.cisco.com.

W okienku Szczegóły pakietu zwróć uwagę na to, że pakiet zawiera Ethernet II, Internet Protocol w wersji 4, User Datagram Protocol i Domain Name System (kwerenda).

Jaki jest źródłowy i docelowy adres MAC? Z którymi interfejsami sieciowymi są skojarzone te adresy MAC?

W tym przykładzie źródłowy adres MAC jest powiązany z kartą sieciową komputera, a docelowy adres MAC jest powiązany z bramą domyślną. Jeśli istnieje lokalny serwer DNS, docelowym adresem MAC będzie adres MAC lokalnego serwera DNS.

Rozwiń Protokół internetowy w wersji 4. Obserwuj adres źródłowy i docelowy

Jaki jest źródłowy i docelowy adres IP? Z którymi interfejsami sieciowymi są skojarzone te adresy IP?

W tym przykładzie źródłowy adres IP jest powiązany z kartą sieciową komputera, a docelowy adres IP jest powiązany z serwerem DNS.

Rozwiń User Datagram Protocol. Obserwuj porty źródłowy i docelowy.

Jaki jest źródłowy i docelowy port? Jaki jest domyślny numer portu DNS?

Numer portu źródłowego to 58461, a port docelowy to 53, co jest domyślnym numerem portu DNS.

Open a Command Prompt and enter arp –a and ipconfig /all to record the MAC and IP addresses of the PC.

```
> arp -a

Interface: 192.168.1.10 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           cc-40-d0-18-a6-81     dynamic
  192.168.1.122         b0-a7-37-46-70-bb     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Studuent> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-80-91-DB
   DHCP Enabled. . . . . . . . . . . : Yes
```

```
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)
    IPv4 Address. . . . . . . . . . . : 192.168.1.10(Preferred)
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Lease Obtained. . . . . . . . . . : Tuesday, August 20, 2019 5:39:51 PM
    Lease Expires . . . . . . . . . . : Wednesday, August 21, 2019 5:39:50 PM
    Default Gateway . . . . . . . . . : 192.168.1.1
    DHCP Server . . . . . . . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . . . . . . . : 50855975
    DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
    DNS Servers . . . . . . . . . . . : 68.105.28.16
                                        68.105.29.16
    NetBIOS over Tcpip. . . . . . . . : Enabled
```

Porównaj adresy MAC i IP w wynikach Wireshark z wynikami `ipconfig /all` . Co można zaobserwować?

Adresy IP i MAC przechwycone w wynikach programu Wireshark są takie same, jak adresy wymienione w poleceniu arp – a i ipconfig /all.

Rozwiń węzeł System nazw domen (kwerenda) w okienku Szczegóły pakietu. Następnie rozwiń Flagi i zapytania.

Zaobserwuj wyniki. Flaga jest ustawiona do wykonywania zapytania rekurencyjnie o adres IP do www.cisco.com.

Krok 3: Przeglądanie odpowiedzi DNS

Wybierz odpowiedni pakiet DNS odpowiedzi oznaczony jako Standardowa odpowiedź zapytania 0x0002 A www.cisco.com.

Jakie są źródłowe i docelowe adresy MAC i IP oraz numery portów? Jak porównać je z adresami w pakietach zapytań DNS?

Źródłowy adres IP, adres MAC i numer portu w pakiecie zapytania są teraz adresami docelowymi. Docelowy adres IP, adres MAC i numer portu w pakiecie zapytania są teraz adresami źródłowymi.

Rozwiń węzeł System nazw domen (odpowiedź). Następnie rozwiń flagi, zapytania i odpowiedzi. Zaobserwuj wyniki.

Czy serwer DNS może wykonywać rekursywne zapytania?

Tak, DNS może obsługiwać zapytania rekurencyjne.

Obserwuj rekordy CNAME i A w szczegółach odpowiedzi.

Jak wypada porównanie wyników z wynikami nslookup?

Wyniki w Wireshark powinny być takie same, jak wyniki nslookup w wierszu poleceń.

Packet Tracer - Demonstracja działania listy ACL

Część 1: Weryfikacja lokalnego połączenia i testowanie listy kontroli dostępu

Krok 1: Użyj komendy ping do urządzeń znajdujących się w sieci lokalnej aby sprawdzić komunikację.

a) W wierszu poleceń komputera PC1 wykonaj ping do komputera PC2.

b) W wierszu poleceń komputera PC1 wykonaj ping do komputera PC3.

Dlaczego test ping się powiódł?

Ponieważ warstwy od 1 do 3 są w pełni funkcjonalne i nie ma obecnie żadnej polityki filtrującej komunikaty ICMP pomiędzy dwiema sieciami lokalnymi.

Krok 2: Użyj komendy ping do urządzeń znajdujących się w sieciach zdalnych by sprawdzić działanie ACL.

a) W wierszu poleceń komputera PC1 wykonaj ping do komputera PC4.

b) W wierszu poleceń komputera PC1 wykonaj ping do komputera DNS Server.

Dlaczego test ping nie powiódł się? (Wskazówka: Użyj trybu symulacji lub wyświetl konfiguracje routera, aby to zbadać).

Pingi nie powiodą się, ponieważ R1 jest skonfigurowany z listą ACL, która uniemożliwia pakietom ping wychodzącym z interfejsu Serial 0/0/0.

Część 2: Usuń listę ACL i powtórz test

Krok 1: Aby zbadać konfigurację ACL, użyj komend show.

a) Przejdź do interfejsu wiersza polecenia R1. Użyj komend show run i show access-lists aby wyświetlić aktualnie skonfigurowane listy ACL. Użyj komendy show access-lists, aby szybko wyświetlić aktualne listy ACL. Wpisz komendę show access-lists a następnie spację i znak zapytania (?), aby wyświetlić dostępne opcje:

```
R1# show access-lists ?
  <1-199> ACL number
  WORD ACL name
  <cr>
```

Jeżeli znasz numer lub nazwę listy ACL, to możesz filtrować wyjście komendy show. Aczkolwiek R1 ma tylko jedną listę ACL; w związku z tym komenda show access-lists jest wystarczająca.

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

Pierwszy wiersz listy ACL blokuje wszystkie pakiety pochodzące z sieci 192.168.10.0/24, która obejmuje echa protokołu ICMP (Internet Control Message Protocol) (żądania ping). Druga linia listy ACL zezwala na cały ruch IP z dowolnego (any) źródła przez router.

b) Aby ACL wpłynęło na działanie routera, musi być zastosowana na interfejsie w określonym kierunku. W tym scenariuszu lista ACL jest używana do filtrowania ruchu wychodzącego interfejsem. W związku z tym cały ruch opuszczający określony interfejs R1 będzie sprawdzany pod kątem listy ACL 11.

Można wyświetlić informacje dotyczące protokołu IP za pomocą komendy show ip interface , ale lepsze jest po prostu użycie polecenia show run. Aby uzyskać pełną listę interfejsów, do których można zastosować listę ACL, oraz listę wszystkich skonfigurowanych list ACL, należy użyć następującego polecenia:

```
R1# show run | include interface|access
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface Serial0/0/0
 ip access-group 11 out
interface Serial0/0/1
interface Vlan1
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
```

Drugi symbol „|" tworzy warunek OR, który pasuje do 'interface' LUB 'access '. Ważne jest, aby żadne spacje nie były uwzględniane w warunku OR. Użyj jednego lub obu tych poleceń, aby znaleźć informacje na temat listy ACL.

Do jakiego interfejsu i w jakim kierunku zastosowana jest ACL?

`Serial 0/0/0, outgoing traffic.`

Krok 2: Usuń listę ACL 11 z konfiguracji.

Do usuwania list ACL z konfiguracji służy komenda no access list [number of the ACL]. Polecenie no access-list używane bez argumentów powoduje usunięcie wszystkich list ACL skonfigurowanych na routerze. Polecenie no access-list [number of the ACL] usuwa tylko określoną listę ACL. Usunięcie listy ACL z routera nie powoduje usunięcia listy ACL z interfejsu. Polecenie, które stosuje ACL do interfejsu, musi zostać usunięte oddzielnie.

a) Na interfejsie Serial0/0/0 usuń listę dostępu 11, która została wcześniej zastosowana do interfejsu jako filtr wychodzący:

```
R1(config)# interface s0/0/0
R1(config-if)# no ip access-group 11 out
```

b) Aby usunąć listę ACL, w trybie konfiguracji globalnej wpisz następującą komendę:

```
R1(config)# no access-list 11
```