Computer Networking

فعالیت نمره اضافه درس شبکه های کامپیوتری

دکتر یغمائی مقدم

Wireshark یک ابزار قدرتمند است که به ما این امکان را می‌دهد تا پیکربندی بسته های ارسالی و دریافتی در شبکه را بررسی کنیم. با انجام این فعالیت به شناخت عمیق‌تری از نحوه کار DNS و DHCP پی خواهید برد و با تحلیل بسته‌های شبکه، اطلاعات ارزشمندی از تبادل داده‌های شبکه به دست خواهید آورد.
در هر مرحله، به سوالات پاسخ مناسب دهید.

مرحله ۱: DNS

1. what is DNS?
2. provide an overview of the command '*nslookup*'.
3. Do the following practices and then write down the results.

    1) Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?
    2) Run *nslookup* to determine the authoritative DNS servers for a university in Europe.
    3) Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

4. provide an overview of the command '*ipconfig*'.
5. Do the following steps then answer the question.

    1) Obtain your IP Address with ipconfig.
    2) Open Wireshark and enter "ip.addr == your_IP_address" into the filter.

3) Start packet capture in Wireshark.
4) With your browser, visit the Web page: http://www.ietf.org
5) Stop packet capture.

Questions:

1) Locate the DNS query and response messages. Are then sent over UDP or TCP?
2) What is the destination port for the DNS query message? What is the source port of DNS response message?
3) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
4) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5) Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

مرحله ۲: DHCP

1. what is DHCP?
2. In order to observe DHCP in action, you have to perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

1) Begin by opening the Windows Command Prompt application. Enter "*ipconfig /release*". The executable for *ipconfig* is in C:\windows\system32. This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.
2) Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
3) Now go back to the Windows Command Prompt and enter "ipconfig /renew". This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 192.168.1.108
4) Wait until the "ipconfig /renew" has terminated. Then enter the same command "ipconfig /renew" again.
5) When the second "ipconfig /renew" terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
6) Finally, enter "ipconfig /renew" to again be allocated an IP address for your computer.
7) Stop Wireshark packet capture.

3. To see only the DHCP packets, in the Wireshark, enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the Wireshark, you need to enter "bootp" and not "dhcp" in the filter.)

4. Answer the following questions:

1) Are DHCP messages sent over UDP or TCP?
2) Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?
3) What is the link-layer (e.g., Ethernet) address of your host?
4) What values in the DHCP discover message differentiate this message from the DHCP request message?

5) What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
6) A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
7) What is the IP address of your DHCP server?
8) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
9) Explain the purpose of the router and subnet mask lines in the DHCP offer message.
10) Explain the purpose of the lease time. How long is the lease time in your experiment?
11) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

موارد قابل توجه

- فعالیت به صورت انفرادی پیاده سازی کنید.
- برای تحویل فعالیت گزارش (document) مناسب تهیه کنید. (این گزارش باید شامل اسکرین شات های مناسب برای پاسخ به سوالات باشد)