**INFO 46206**

**Assignment 2: TCPdump Filters**

|  |  |
| --- | --- |
| Student Names: | Kevin Harianto |
| Class day/time: | February 6th 2023 |

**Instructions:**

* For each scenario below, enter the TCPdump filter you would use to get the required packets. Submit the file in SLATE before the deadline.
* When writing filters for TCP flags, **DO NOT** use this kind of filter: tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0.   
  Instead use tcp[13] and bit masks as shown in class.
* Make sure the entire tcpdump filter is enclosed in single quotes. For example: tcpdump 'host 1.2.3.4 and port 80'
* Example Question: Match packets where the source address is 10.1.1.1.   
  Answer format: \*\*\* \*\*\*\* \*\*.\*.\*.\*  
  Answer: src host 10.1.1.1
* Part 1: Each question below is worth **1 point**.

|  |
| --- |
| 1. Match packets where the destination IP address is 10.10.0.24. If you test your filter with the file BA you will get one match (ip id 39426).   Answer format: \*\*\* \*\*\*\* \*\*.\*\*.\*.\*\* |
| dst host 10.10.0.24 |
| 1. Match traffic involving TCP port 80 (whether it is source or destination)   Answer format: \*\*\* \*\*\*\* \*\* |
| tcp port 80 |
| 1. Match traffic where the destination TCP port is 80. File DG1 has one match (id 7302).   Answer format: \*\*\* \*\*\* \*\*\*\* \*\* |
| tcp dst port 80 |
| 1. Match Ethernet frames where the destination MAC address is 00:00:0A:12:34:56.   Answer format: \*\*\*\*\* \*\*\* \*\*\*\* \*\*:\*\*:\*\*:\*\*:\*\*:\*\* |
| ether dst host 00:00:0A:12:34:56 |

* Part 2: Each question below is worth **2 points**.

|  |
| --- |
| 1. Match TCP segments where only the SYN and FIN flags are set to 1. File BA has many matches.   Answer format: \*\*\*\*\*\*\* \* \*\*\*\* |
| tcp[13] = 0x12 |
| 1. Match TCP segments where the SYN and FIN flags are set to 1 (regardless of the other flags). File DG3 has one match (id 7272).   Answer format: \*\*\*\*\*\*\* \* \* = \* |
| tcp[13] & 3 = 3 |
| 1. Match TCP segments that represent step #2 in the 3-way handshake. File BA has one match. (id 0)   Answer format: \*\*\*\*\*\*\* = \*\*\*\* Alternative answer format: \*\*\*\*\*\*\* = \*\* |
| tcp[13] = 18 |
| 1. Match TCP segments where the sequence number is 0.  File DG3 has one match. (id 7272)   Answer format: \*\*\*\*\*:\*\* \* \* |
| tcp[4:4] = 0 |
| 1. Match TCP segments where the ACK flag is set and the ACK number is 0. File DG1 will have a match for this filter. (id 7302)   Answer format: \*\*\*\*\*\*\* \* \*\*\*\* \* \*\*\*\* and \*\*\*\*\*:\*\* \* \* |
| tcp[13] & 0x10 = 0x10 and tcp[8:4] = 0 |
| 1. Match TCP segments that have optional fields in the TCP header. File BA has 4 matches.   Possible answer formats: \*\*\*\*\*\*\* \*\* \* \* \* \*\*\*\*\*\*\* \* \*\* \* \* \*\*\*\*\*\*\* \* \*\*\*\* \*\*\*\*\*\*\* \*\* \*\*\*\* |
| tcp[12] >> 4 > 5 |

* Part 3: Each question below is worth **2 points**.

|  |
| --- |
| 1. Match ICMP "Fragment reassembly time exceeded" error messages. File DG2 has one match. (id 12512)   Possible answer formats:  \*\*\*\*\*\*\* \* \*\* and \*\*\*\*\*\*\* \* \* \*\*\*\*\*\*:\*\* \* \*\*\*\*\*\* |
| icmp[1] = 11 and icmp[0] = 3 |
| 1. Match IP packets where the TTL value in the IP header is less than 10. File DG1 has one match. (id 58235)   Answer format: \*\*\*\*\* \* \*\* |
| ip[8] < 10 |
| 1. Match IP packets where the 3rd octet in the destination IP address is 164. File BA has one match. (id 13031)   Answer format: \*\*\*\*\*\* \* \*\*\* |
| ip[18] = 164 |
| 1. Match IP packets carrying DCCP messages (protocol number 33). File DG2 has one match (id 16857).   Answer format: \*\*\*\*\* \* \*\* |
| ip[9] = 33 |
| 1. Match IP packets that are the last fragment in a fragment train. File DG1 has one match (id 18761).   Answer format: \*\*\*\*\* \* 0x\*\* \* \* and \*\*\*\*\*\*\* \* 0x\*\*\*\* \*\* \* |
| ip[6] & 0x1f = 0 and ip[6:2] & 0x2000 != 0 |
| 1. Match IPv4 packets where the version field is not equal to 4. File DG2 has one match (id 0x1c86).   Possible answer formats: \*\*\*\*\* \*\* \* \*\* \* \*\*\*\*\* \* \*\*\*\* \*\* \*\*\*\* |
| ip[0] >> 4 != 4 |
| 1. Match IP packets where the IP header contains optional fields.   Answer format: \*\*\*\*\* \* \*\*\*\* \* \* |
| ip[0] & 0x0f > 5 |
| 1. Match IP packets with a non-zero fragment offset. File DG1 has one match (id 18761). File DG2 has 4 matches.   Answer format: \*\*\*\*:\*\* \* 0x\*\*\*\* \*\* \* |
| ip[6:2] & 0x1fff != 0 |
| 1. Match UDP traffic where the source and destination ports are the same. File DG2 has 2 matches.   Answer format: \*\*\*\*\*\*\*\* \* \*\*\*\*\*\*\*\* |
| udp[0:2] = udp[2:2] |