Information Assurance and Security (IT352) Lab Program-3
For Reg. No 181560181IT245, 191300191IT101-191023191IT212

Use any one of the programming languages such as C/C++/Java/Python to implement one of the basic concepts of Network Based-Intrusion Detection Technique. Your program should consider the run-time input file (.csv) and it should consider entire row as one packets; it should read entire row one at a time to check the following to declare the read packet as intrusion related packet:

- Both Source and Destination address are same
- Either Source or Destination Address is broadcast address (all are 1111…111).
- Byte count less than 40
- Protocol is ICMP

If any one of the above-mentioned conditions is satisfied then print the following on the terminal that "*Analyzed Packet is Intrusion Packet*" followed by entire packet on the next line. Furthermore, print the following after completion of checking of entire run-time input file: total number of packets checked is = , total number of intrusion packets detected is = .

If none the conditions mentioned in the previous slide is satisfied then print the following the terminal that "*Analyzed Packet is Not-Intrusion Packet*" followed by entire packet on the next line. Furthermore, print the following after completion of checking of entire run-time input file: total number of packets checked is =, total number of intrusion packets detected is = . Store the output of the program on the output file also.

Sample Text Cases

1. Sample-Testcase-1.csv
2. Sample-Testcase-2.csv

File name of the program : RegisterNo_IT352_P3

(P3 indicates Lab Program Number-3)

File name of the screenshot : RegisterNo_IT352_P3_TCS1

(TCS1 indicates screenshot for the first test case, similarly, for other test cases TCS2, TCS3, TCS4, TC5, TC6)

File name of the Output File : RegisterNo_IT352_P3_Output_TC1.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC5, TC6)

Date of Online Laboratory : 9th February 2022, Wednesday

Deadline of Submission : 12th February 2022, Saturday on or before 6:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-3-Submisison Web Link*".

Information Assurance and Security (IT352) Lab Program-3
For Reg. No 191IT213 - 191IT258

Use any one of the programming languages such as C/C++/Java/Python to implement one of the basic concepts of Network Based-Intrusion Detection Techniques. Your program should consider the run-time input file (.pacp) and it should only consider first "N" number of packets exit in the give .pcap file, it should consider one packet at a time to check the following to declare the read packet as intrusion related packet:

- Both Source and Destination address are same
- Either Source or Destination Address is broadcast address (all are 1111…111).
- Protocol is ICMP

If any one of the above mentioned conditions is satisfied then print the following on the terminal that "*Analyzed Packet is Intrusion Packet*" followed by entire packet on the next line. Furthermore, print the following after completion of checking of entire run-time input file: total number of packets checked is =, the number of intrusion packets detected is = . If none the conditions mentioned in the previous slide is satisfied then print the following the terminal that "*Analyzed Packet is Not-Intrusion Packet*" followed by entire packet on the next line. Furthermore, print the following after completion of checking of entire run-time input file: total number of packets checked is =, total number of intrusion packets detected is = . Store the output of the program on the output file also.

Sample Text Cases

1. N=35, Sample-Testcase.pcap

File name of the program : RegisterNo_IT352_P3

(P3 indicates Lab Program Number-3)

File name of the screenshot : RegisterNo_IT352_P3_TCS1

(TCS1 indicates screenshot for the first test case, similarly, for other test cases TCS2, TCS3, TCS4, TC5, TC6)

File name of the Output File : RegisterNo_IT352_P3_Output_TC1.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC5, TC6)

Date of Online Laboratory : 9th February 2022, Wednesday

Deadline of Submission : 12th February 2022, Saturday on or before 6:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-3-Submisison Web Link*".

Note : No/Zero marks for incomplete submission/late submission/incomplete program. No email submission is considered for evaluation.