IT352: INFORMATION ASSURANCE AND SECURITY

LAB 3 – Packet Sniffing and applying ACL Rules

10th Feb 2021

Submitted by: Harsh Agarwal (181IT117)

Testcase 1:

- Use 20.20.20.20, 100.100.100.100 as source IP address and destination IP address, respectively. Use source port as 11, destination port as 80.
- Use these details with sr1() function to craft the packet and send the crafted packet in real-time.
- Use Destination IP as 100.100.100.100 to set the filter option in sniff() function.

Output:

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python 181IT117_IT352_Lab3.py
Enter the Test Case Number: 1
Sniffing ..........................


Raw Packet:
b'f\xa7\xb7|\x1a\x02\xe8*D}\x8dq\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06\x89\xdf\x14\x14\x14\x14dddd\x00\x0b\x00P\x00\x00
\x00\x00\x00\x00\x00\x00\x00P\x02 \x00\x9e\x97\x00\x00'

Packet in hexadecimal format:
 66 a7 b7 7c 1a 02 e8 2a 44 7d 8d 71 08 00 45 00 00 28 00 01 00 00 40 06 89 df 14 14 14 14 64 64 64 64 00 0b 00 50 00 00
 00 00 00 00 00 00 50 02 20 00 9e 97 00 00


Protocol          :TCP
Version           : 4
IHL               : 5

Source MAC: e8:2a:44:7d:8d:71
Destination MAC: 66:a7:b7:7c:1a:02

Source IP: 20.20.20.20
Source Port: 11
Destination IP: 100.100.100.100
Destination Port: 80

ACL Rule Applied   : ['10.10.1.1', 'Any', 'Any', '80', 'Deny']


Result : ALLOW

$
```

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python tc1.py
Begin emission:
Finished sending 1 packets.
.....................................................................................
```

RESULT: ALLOW THE PACKET

Testcase 2:

- Use 200.200.200.200, 100.100.110.100 as source IP address and destination IP address, respectively. Use source port as 81, destination port as 400.
- Use these details with srloop() function to craft the packet and send the crafted packet in real-time.
- Use Destination IP as 100.100.110.100 to set the filter option in sniff() function.

Output:

```
MINGW64:/d/Academics/6th Sem/Information Security/Labs/Lab3/Program

$ python 181IT117_IT352_Lab3.py
Enter the Test Case Number: 2
Sniffing ..........................


Raw Packet:
b'f\xa7\xb7|\x1a\x02\xe8*D}\x8dq\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06\x16v\xc8\xc8\xc8\xc8ddnd\x00Q\x01\x90\x00\x00\x0
0\x00\x00\x00\x00\x00P\x02 \x00)\xa8\x00\x00'

Packet in hexadecimal format:
 66 a7 b7 7c 1a 02 e8 2a 44 7d 8d 71 08 00 45 00 00 28 00 01 00 00 40 06 16 76 c8 c8 c8 c8 64 64 6e 64 00 51 01 90 00 00
 00 00 00 00 00 00 50 02 20 00 29 a8 00 00


Protocol          :TCP
Version           : 4
IHL               : 5

Source MAC: e8:2a:44:7d:8d:71
Destination MAC: 66:a7:b7:7c:1a:02

Source IP: 200.200.200.200
Source Port: 81
Destination IP: 100.100.110.100
Destination Port: 400

ACL Rule Applied   : ['Any', 'Any', '100.100.100.100', '80', 'Deny']


Result : ALLOW

harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$
```

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python tc2.py
Begin emission:
Finished sending 1 packets.
.....................................................................................
.....................................................................................
```

RESULT: ALLOW THE PACKET

Testcase 3:

- Use 20.20.20.20, 200.200.200.200 as source IP address and destination IP address, respectively. Use source port as 81, destination port as 80. Use these details with sr() function to craft the packet and send the crafted packet in real-time.
- Use Destination IP as 200.200.200.200 to set the filter option in sniff() function.

Output:

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python 181IT117_IT352_Lab3.py
Enter the Test Case Number: 3
Sniffing ..........................


Raw Packet:
b'f\xa7\xb7|\x1a\x02\xe8*D}\x8dq\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06\xc1\x16\x14\x14\x14\x14\xc8\xc8\xc8\xc8\x00Q\x00
P\x00\x00\x00\x00\x00\x00\x00\x00P\x02 \x00\xd5\x88\x00\x00'

Packet in hexadecimal format:
 66 a7 b7 7c 1a 02 e8 2a 44 7d 8d 71 08 00 45 00 00 28 00 01 00 00 40 06 c1 16 14 14 14 14 c8 c8 c8 c8 00 51 00 50 00 00
 00 00 00 00 00 00 50 02 20 00 d5 88 00 00


Protocol           :TCP
Version            : 4
IHL                : 5

Source MAC: e8:2a:44:7d:8d:71
Destination MAC: 66:a7:b7:7c:1a:02

Source IP: 20.20.20.20
Source Port: 81
Destination IP: 200.200.200.200
Destination Port: 80

ACL Rule Applied   : ['Any', 'Any', '100.100.110.100', '400', 'Deny']


Result : ALLOW

harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
```

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python tc3.py
Begin emission:
Finished sending 1 packets.
```

RESULT: ALLOW THE PACKET

Testcase 4:

- Use 200.20.202.20, 100.102.100.102 as source IP address and destination IP address, respectively. Use source port as 81, destination port as 80. Use these details with srloop() function to craft the packet and send the crafted packet in real-time.
- Use Destination IP as 100.102.100.102 to set the filter option in sniff() function.

Output:

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python 181IT117_IT352_Lab3.py
Enter the Test Case Number: 4
Sniffing ..........................


Raw Packet:
b'f\xa7\xb7|\x1a\x02\xe8*D}\x8dq\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06\x1f\xda\xc8\x14\xca\x14dfdf\x00Q\x00P\x00\x00\x00\x00\x00\x00\x00\x00P\x02 \x004L\x00\x00'

Packet in hexadecimal format:
 66 a7 b7 7c 1a 02 e8 2a 44 7d 8d 71 08 00 45 00 00 28 00 01 00 00 40 06 1f da c8 14 ca 14 64 66 64 66 00 51 00 50 00 00
 00 00 00 00 00 00 50 02 20 00 34 4c 00 00


Protocol            :TCP
Version             : 4
IHL                 : 5

Source MAC: e8:2a:44:7d:8d:71
Destination MAC: 66:a7:b7:7c:1a:02

Source IP: 200.20.202.20
Source Port: 81
Destination IP: 100.102.100.102
Destination Port: 80

ACL Rule Applied    : ['Any', 'Any', '200.200.200.200', 'Any', 'Deny']


Result : ALLOW

harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
```

```
harsh@EDUCATION MINGW64 /d/Academics/6th Sem/Information Security/Labs/Lab3/Program
$ python tc4.py
Begin emission:
Finished sending 1 packets.
.................
```

RESULT: ALLOW THE PACKET