

# IT352: INFORMATION ASSURANCE AND SECURITY

## LAB 2 – Packet Sniffing and applying ACL Rules

Submitted by: Harsh Agarwal (181IT117)

### Testcase 1:

#### Ethernet Frame:

50 eb 1a 90 61 32 6c c2 17 77 00 a6 08 00 45 00 00 29 1f 54 40 00 80 06 31 8a 0a 64  
35 7b 36 48 33 ca 07 9d 20 5a 49 6c d0 2e 09 c1 e2 98 50 10 00 fb d6 fb 00 00 00

#### Output:

```

C:\> MINGW64:/d/Academics/6th Sem/Information Security/Labs/Lab2
$ python 181IT117_IT352_Lab2.py

-----Testcase # 1 -----

Version: 4
Protocol: 06

Source MAC: 6c:c2:17:77:00:a6
Destination MAC: 50:eb:1a:90:61:32

Source IP: 10.100.53.123
Source Port: 1949
Destination IP: 54.72.51.202
Destination Port: 8282
ACL Rule Applied: ['10.100.54.*', 'Any', 'Any', 'Any', 'Allow']

Result: DENY
```

### Testcase 2:

#### Ethernet Frame:

6c c2 17 77 00 a6 50 eb 1a 90 61 32 08 00 45 00 00 34 98 af 40 00 e9 06 4f 23 36 48  
33 ca 0a 64 35 7b 20 5a 07 9d 09 c1 e2 98 49 6c d0 2f 80 10 01 a6 6d 02 00 00 01 01  
05 0a 49 6c d0 2e 49 6c d0 2f

#### Output:

-----Testcase # 2 -----

Version: 4

Protocol: 06

Source MAC: 50:eb:1a:90:61:32

Destination MAC: 6c:c2:17:77:00:a6

Source IP: 54.72.51.202

Source Port: 8282

Destination IP: 10.100.53.123

Destination Port: 1949

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

Result: ALLOW

### **Testcase 3:**

#### Ethernet Frame:

ff ff ff ff ff 30 9c 23 50 ce c0 08 00 45 00 00 44 73 0e 00 00 80 11 85 ad 0a 64 37 8a ff  
ff ff ff f2 1c 07 9b 00 30 de 69 50 6b 70 36 70 74 64 49 37 71 7a 49 4a 46 6b 55 33 47  
79 61 58 67 75 36 65 51 7a 64 39 54 70 6e 30 43 2f 51 38 34 4d 41

#### Output:

MINGW64:/d/Academics/6th Sem/Information Security/Labs/Lab2

-----Testcase # 3 -----

Version: 4

Protocol: 11

Source MAC: 30:9c:23:50:ce:c0

Destination MAC: ff:ff:ff:ff:ff:ff

Source IP: 10.100.55.138

Source Port: 61980

Destination IP: 255.255.255.255

Destination Port: 1947

ACL Rule Applied: ['Any', 'Any', '10.100.53.1', '443', 'Deny']

Result: ALLOW

#### **Testcase 4:**

##### Ethernet Frame:

50 eb 1a 90 61 32 6c c2 17 77 00 a6 08 00 45 00 00 29 73 0b 40 00 80 06 ac 4d 0a 64  
35 7b 0d 21 8e 76 09 13 01 bb 1c 8d 82 1c 6b 7b 7f e1 50 10 00 fe 3e 8b 00 00

##### Output:


```
-----Testcase # 4 -----  
  
Version: 4  
Protocol: 06  
  
Source MAC: 6c:c2:17:77:00:a6  
Destination MAC: 50:eb:1a:90:61:32  
  
Source IP: 10.100.53.123  
Source Port: 2323  
Destination IP: 13.33.142.118  
Destination Port: 443  
ACL Rule Applied: ['Any', 'Any', '10.100.54.*', 'Any', 'Deny']  
  
Result: ALLOW
```

#### **Testcase 5:**

##### Ethernet Frame:

6c c2 17 77 00 a6 50 eb 1a 90 61 32 08 00 45 00 00 34 c0 eb 40 00 3f 06 9f 62 0d 21  
8e 76 0a 64 35 7b 01 bb 09 13 6b 7b 7f e1 1c 8d 82 1d 80 10 00 f5 cb 28 00 00 01 01  
05 0a 1c 8d 82 1c 1c 8d 82 1d

##### Output:

 MINGW64:/d/Academics/6th Sem/Information Security/Labs/Lab2

-----Testcase # 5 -----

Version: 4

Protocol: 06

Source MAC: 50:eb:1a:90:61:32

Destination MAC: 6c:c2:17:77:00:a6

Source IP: 13.33.142.118

Source Port: 443

Destination IP: 10.100.53.123

Destination Port: 2323

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

Result: DENY