EL5373

INTERNET ARCHITECTURE AND PROTOCOLS

Zheng Pan

0495069

zp322@students.poly.edu

workstation: APAH

MAC: 00:16:76:a9:82:01

Lab Report 9

Due 8 March 2013

[5 Pages]

Exercise 1

In this lab, community name is guest.
Community name defines the access scope for SNMP managers and agents. An SNMP message carrying a different community name is discarded. This provides a simple authentication for the SNMP messages.
The data type for the MIB object ifMtu.2 is Integer32.
The definition of the MIB object ifPhysAddress and ifInOctets
ifPhysAddress is the interface's address at its protocol sub-layer. For example, for an 802.x interface, this object normally contains a MAC address. The interface's media-specific MIB must define the bit and byte ordering and the format of the value of this object. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length."
ifInOctets is the total number of octets received on the interface, including framing characters.
The data type of tcpRto Algorithm is Integer. The algorithm used to determine the timeout value used for retransmitting unacknowledged octets. Values that are allowed for tcpRtoAlgorithm are 1, 2, 3, 4.
tcpMaxConn:the limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Exercise 2

```
[guest@apah guest]$ snmpwalk -v 2c -c guest localhost interface
IF-MIB::ifNumber.0 = INTEGER: 2
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 16436
IF-MIB::ifMtu.2 = INTEGER: 1500
```

MTU of the Ethernet interface is 1500 and MTU of the loopback interface is 16436

```
[guest@apah guest]$ netstat -i
Kernel Interface table
Iface      MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500   0       40      0      0      0        5      0      0      0
BMRU
lo       16436   0    11321      0      0      0    11321      0      0      0
LRU
```

The snmpwalk command with a community name public fail, because in the lab we have configured the community name as guest not the default name public.

Exercise 3

The port number used by the SNMP agent is 161.
The full text-based and numerical object ID of the MIB object interface.ifMTU.1 is 1.3.6.1.2.1.2.2.1.4.1.
The value returned is 16436.

Version Number	Community Name	PDU Type	Request ID	Error Status	Error Index	Object1	Value1
v2c(1)	guest	get	1846533288	noError(0)	0	1.3.6.1.2.1.2.2.1.4.1	16436

Exercise 4

I can see the login ID and the password in the FTP.

```
⊞ Transmission Control Protocol, Src P
⊟ File Transfer Protocol (FTP)
  ⊟ USER 1111\r\n
      Request command: USER
      Request arg: 1111
```

```
⊟ File Transfer Protocol (FTP)
  ⊟ PASS 2222\r\n
      Request command: PASS
      Request arg: 2222
```

I can see the login ID and the password in the telnet.

```
⊟ Telnet
    Data: login:
```

```
⊟ Telnet
    Data: 1
```

```
⊟ Telnet
    Data: 1
```

```
⊟ Telnet
    Data: 1
```

```
⊟ Telnet
    Data: 1
```

```
⊟ Telnet
    Data: Password:
```

```
⊟ Telnet
    Data: 2
```

FTP sends user ID's in one packet and so are passwords. Telnet sends user ID's one character in one packet. So are passwords.
They do not have any built-in security measures. Even usernames and passwords are sent in plain text, making them vulnerable to sniffing. But comparing these two, telnet is more secure.

Exercise 5

I cannot extract the password from the tcpdump output.
I can read the IP, TCP and SSH header, but can't read the TCP data.
The client uses SSH and SSHv2 in both cases.
Port 22 is used by the SSH server.
Port 22 is used by the SFTP server.

Exercise 8

I cannot telnet the host from the remote machine.
Telnet makes 6 reties.
TCP uses the Exponential Backoff algorithm to update RTO when the retransmission timer expires for a retransmitted segment. RTO is doubled for each retransmission, but with a maximum value of 64 seconds.

Exercise 9

The difference is that in this experiment TCP does not retry. Drop option means iptables drops the packet without notifying the sender, but the reject option means that the packet will be dropped and will also return an error message to the sender. In this lab, a reset message is returned. So the sender will not retransmit the packet. Only one attempt did TCP make this time.

Exercise 12

```
.............
daytime-udp:    off
       daytime:         off
       echo-udp:        on
       echo:      on
```

```
        services:       off
        servers:        off
        time-udp:       on
        time:   on
        cups-lpd:       off
        sgi_fam:        on
        finger: off
        ktalk:  off
        rexec:  off
        rlogin: off
        rsh:    off
        ntalk:  off
        talk:   off
  ..............
```

Rlogin is not enabled.