Network Lab Kevin Neumann & Alain C. Mendy

Lab Report 9

5.1: UDP
5.2: .1.3.6.1.2.1.5
5.3: See files
Ex.3: See files

Ex.4:

a) Version number (version-1) and type of community (public)

b) As a composition of snmpgetnext

c) A practical maximum is the size that can fix in a UDP message that does not cause IP fragmentation. This is around 1200 Octets on Ethernet Networks

d) Plain text seems to be stored in variable bindings in the SNMP message. IP end MAC addresse are encoded in the internet protocol and ethernet layer oft he message

e) The snmpgetnext command requests an object and in response there will also be the object name be transmitted

Ex.5.:

Small differences like the different description. When using the command udp.udpInDatagrams the router and PC had a different counter

Ex.6:

a) Timeout: No response from 10.0.4.14
b) Agent doesn‘t send a response
c) See File Ex6, ex6.wireshark.out

Ex.7:

a) The 12 means delete TCB. Can be found out by using SNMP translate commands
b) It just uses plain text an das such is highly insecure

Ex.8:

α) There are no apperent differences in the message
β) msgFlags, msgAuthorativeEngineID, msgAuthorativeEngineBoots, msgAuthorativeEngineTime, msgUserName, msgAuthenticationParameters
χ) There are several new mesages now: First a get-request, a report as response and then a encypted request and response
δ) See File ex8.wireshark.out

ε) Explain:

- SNMPv1, SNMPv2 (matching community string):

- SNMPv3 (NoAuthNoPriv)
- SNMPv3 (authNoPriv)
- SNMPv3 (authPriv)

ϕ) Give an attack type to which even SNMP even with authPric is vulnerable

Ex.9:

a) File Ex9.wireshark.out
b) coldStart and enterpriseSpecific
c) One for each
d) See files ex9.d.consoleout and ex9.d.wireshark.out
e) enterpriseSpecific, linkDown, linkUp

Ex.10:

a) It uses a kind of „verctor algorithm“ to discover ist next hop.