Date:

EXPERIMENT: 22

TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK- TCP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- TCP

SOFTWARE USED:

Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 → IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for TCP

Date:

EXPERIMENT: 23

TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK- UDP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- UDP.

SOFTWARE USED:

Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 →IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for UDP.

Date:

EXPERIMENT-24

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – SMTP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark-SMTP

SOFTWARE USED:

Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 → IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for SMTP

Date:

EXPERIMENT-25

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – ICMP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark-ICMP.

SOFTWARE USED:

Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 → IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for ICMP.

Date:

EXPERIMENT-26

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – ARP

AIM: To analyze capturing of Transport layer protocol header analysis using Wire shark- ARP

SOFTWARE USED:

Wire shark network analyzer

PROCEDURE:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 →IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for ARP

Date:

EXPERIMENT-27

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – HTTP

AIM: To analyze capturing of Transport layer protocol header analysis using Wire shark-HTTP.

SOFTWARE USED:

Wire shark network analyzer

PROCEDURE:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 →IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for

HTTP.