# Cybersecurity

# **Activity 3.3.2 Analyzing Control Messages**

Copy and paste screenshots and/or answer questions from the activity.

#3 Source: 192.168.100.138

Destination: 4.2.2.1

#6 Source: 192.168.100.1

Destination: 192.168.100.138

How does this compare to the request address? The IP 192.168.100.1 must be a router

#14

|  |  |
| --- | --- |
| icmp\_traceroute: Router IP Addresses | |
| Router 1:  192.168.100.1 | Router 6: 12.122.133.137 |
| Router 2: 12.180.241.1 | Router 7: 192.205.33.210 |
| Router 3: 12.153.21.202 | Router 8: 4.68.101.162 |
| Router 4: 12.86.61.157 | Router 9: |
| Router 5: 12.122.133.110 | Router 10: |

1. How can traceroute help a network administrator?

Check the active connections that a packet of information travels to get to its destination

1. How might it be useful to an attacker?

Listing the systems that data passes through

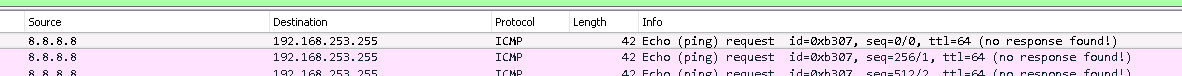
1. What do you think would happen if a router along the path was configured to ignore these kinds of ICMP messages?

The traceroute function or idea would not work

#17 Screenshot of your results

Text

Description automatically generated



#18 Find the fully qualified domain name for the source machine. Do you recognize the source? dns.google

#19 Approximately how many packets were sent from the source to your host and in what amount of time?

Number of Packets: about 81,700 packets

Duration: 2 seconds

Conclusion:

#2 What are the effects of an ICMP reflected (Smurf) attack?

Similar to a ping flood attack but rather spoofs address source so that another host replies to it

#3 How do you protect against an ICMP reflected exploit?

Configure the firewall to drop ICMP requests