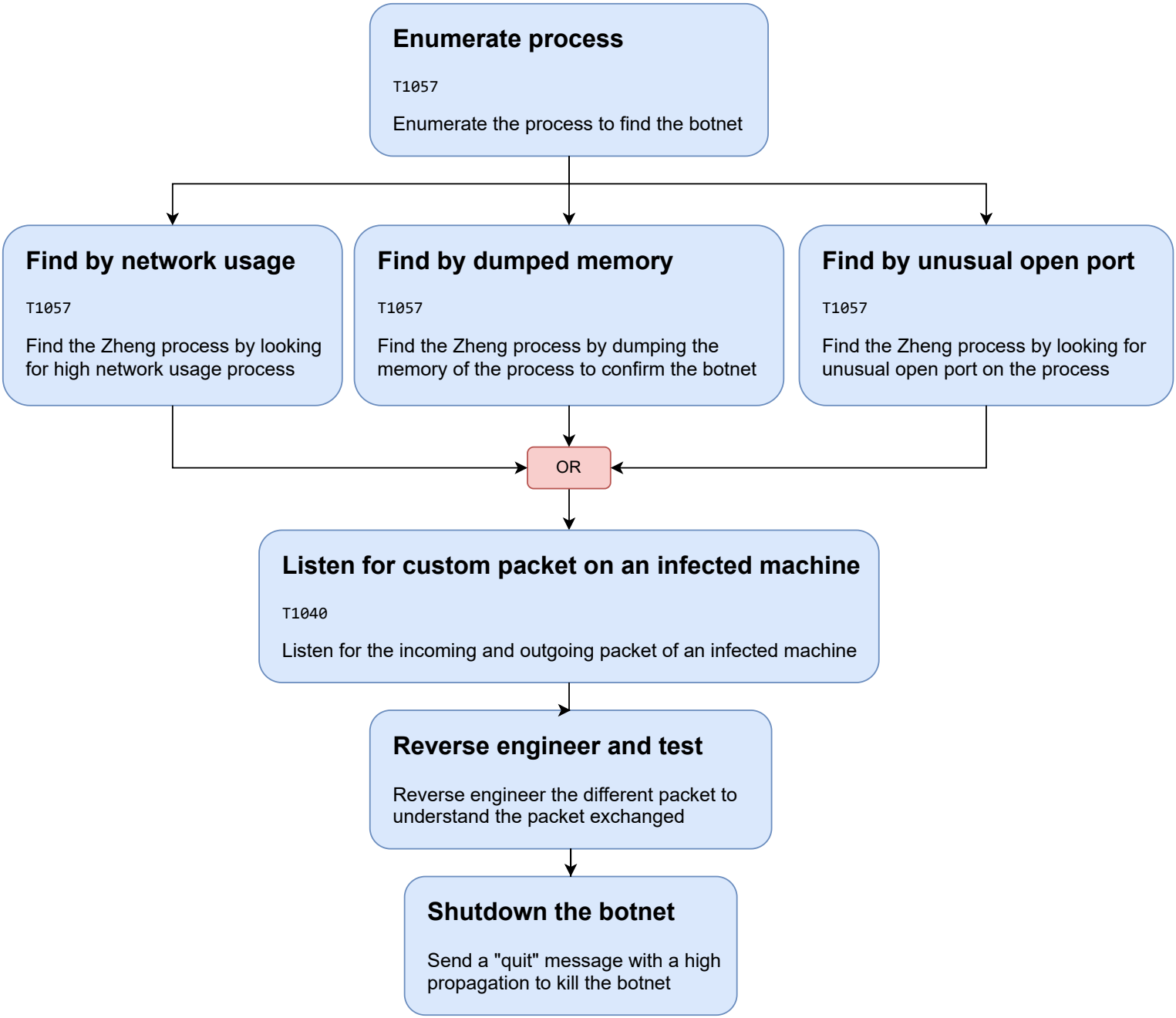
Enumerate process
T1057
Enumerate the process to find the botnet
Find by network usage
T1057
Find the Zheng process by looking for high network usage process
Find by dumped memory
T1057
Find the Zheng process by dumping the memory of the process to confirm the botnet
Find by unusual open port
T1057
Find the Zheng process by looking for unusual open port on the process
OR
Listen for custom packet on an infected machine
T1040
Listen for the incoming and outgoing packet of an infected machine
Reverse engineer and test
Reverse engineer the different packet to understand the packet exchanged
Shutdown the botnet
Send a "quit" message with a high propagation to kill the botnet