**Completing "1. Develop a Splunk query to detect phishing emails containing links to zip files for download, utilizing MITRE ATT&CK T1566.002 and T1204.002 techniques."**

The following is a Splunk query to detect phishing emails containing links to zip files for download, utilizing MITRE ATT&CK T1566.002 and T1204.002 techniques:

index=<insert\_index\_name> sourcetype=<insert\_sourcetype\_name> (file\_name=".zip" OR file\_name=".rar") AND (body="http" OR body="https") AND (body="exe" OR body="js") AND (body="download" OR body="click" OR body="link") AND (body="malicious" OR body="virus" OR body="ransomware") | stats count by src\_ip, dest\_ip, file\_name, body

This query searches for emails that contain links to zip files for download, and also contain keywords related to malicious activity such as "malicious", "virus", or "ransomware". It also looks for keywords related to the execution of malicious files such as "exe" or "js". The query outputs the source IP, destination IP, file name, and body of the email for further investigation.