# Reconnaissance

1.Ping Activities

|  |
| --- |
| index=security\_logs sourcetype=network\_traffic ((method=ping) OR (method=GET OR method=POST AND (uri="/\*" OR uri="/robots.txt" OR uri="/phpMyAdmin/" OR uri="/wp-admin/")))  | stats count by clientip, uri, method  | sort -count |

This query searches the security\_logs index and the network\_traffic sourcetype for events where the HTTP method is either ping, GET, or POST and the URI matches a known reconnaissance path, such as /robots.txt, /phpMyAdmin/, or /wp-admin/. The query then groups the results by client IP address, URI, and HTTP method and sorts them by count in descending order.

2.Nmap Scanning Activities

|  |
| --- |
| index=security\_logs sourcetype=network\_traffic (src\_port=53 AND dest\_port=53 AND (UDP) AND (orig\_fuids=\* OR resp\_fuids=\*))  | rex field=orig\_payload "^\d+\.\d+\.\d+\.\d+"  | stats count by src\_ip  | where count > 10 |

This query searches the security\_logs index and the network\_traffic sourcetype for DNS traffic (source port 53 and destination port 53) over UDP protocol where the FUIDs (File Unique IDs) are present. This indicates that there was actual data exchange instead of just domain resolution. It then extracts the IP address of the client that made the request using regex and groups the results by source IP address. The query then filters out the IP addresses that made more than 10 requests.

Nmap is a tool that can perform host discovery and port scanning, and it often uses DNS queries to identify live hosts. This query searches for DNS traffic that could indicate the use of Nmap for reconnaissance. However, it is important to review the results carefully and investigate any suspicious activity to determine if it is a genuine threat or a false positive. Additionally, there may be other indicators of Nmap scanning activity that could be used to refine the search query further.

1.Malware Attack

|  |
| --- |
| index=security\_logs sourcetype=windows\_security EventCode=4688 "Image File Name"="\*.exe"  | stats count by "Image File Name"  | sort -count  | head 10 |

This search looks for the creation of executable files on Windows systems, which may indicate the presence of malware.

2.Phishing Attack

|  |
| --- |
| index=email\_logs sourcetype=exchange | stats count by sender, subject  | sort -count  | head 10 |

This search looks for email messages sent from suspicious senders with unusual subjects, which may indicate a phishing attack.

3.DDoS Attack

|  |
| --- |
| index=security\_logs sourcetype=windows\_security EventCode=4688 "Image File Name"="\*.exe"  | stats count by "Image File Name"  | sort -count  | head 10 |

This search looks for network traffic spikes that may indicate a DDoS attack. The search calculates the total incoming and outgoing bytes every minute and filters for a total traffic volume of more than 5 MB.

4.Insider Threats

|  |
| --- |
| index=security\_logs sourcetype=windows\_security EventCode=4663 | stats count by User, Object\_Name  | sort -count  | head 10 |

This search looks for attempts to access files or directories that may be sensitive or outside the user's normal scope of access, which may indicate an insider threat.

5.Brute force Attacks

|  |
| --- |
| index=security\_logs sourcetype=windows\_security EventCode=4688 "Image File Name"="\*.exe"  | stats count by "Image File Name"  | sort -count  | head 10 |

This search looks for repeated failed login attempts from a particular IP address, which may indicate a brute force attack.

SQL Injection Attacks

|  |
| --- |
| index=database\_logs | search SQLSTATE="42S02"  | stats count by query, user  | sort -count  | head 10 |

This search looks for errors in SQL statements, which may indicate a SQL injection attack. The search filters for SQLSTATE errors of "42S02", which indicates that the table or view does not exist.