🧠 1. Prerequisites

Before threat hunting in Splunk, ensure:

- Splunk Enterprise or Splunk Cloud is installed.
- You have **logs from endpoints, firewalls, proxies, DNS, authentication servers, and Sysmon**.
- You have **index and sourcetype** properly configured (e.g., index=winlogs, sourcetype=WinEventLog:Security).

⚔️ 2. Threat Hunting Framework: Lockheed Martin Kill Chain

Kill Chain Phase	Splunk Focus	Example Data Sources
Reconnaissance	Unusual access, scanning	Proxy, firewall
Weaponization	File creation, attachments	Email, endpoint
Delivery	File download or email	Proxy, email logs
Exploitation	Exploit execution	Sysmon, EDR
Installation	Registry changes	Sysmon, Windows Logs
C2 (Command & Control)	Beaconing patterns	DNS, proxy
Actions on Objectives	Data exfiltration	DLP, proxy

🔍 3. Basic Threat Hunting Commands

3.1 Authentication Anomalies

Detect multiple failed logins followed by a success:

index=wineventlog sourcetype="WinEventLog:Security"

(EventCode=4625 OR EventCode=4624)

| stats count(eval(EventCode=4625)) as failed count(eval(EventCode=4624)) as success by user, src_ip

| where failed > 5 AND success > 0

| sort - failed

3.2 Privilege Escalation Attempts

Detect creation of new admin users:

```
index=wineventlog EventCode=4720 OR EventCode=4728
| table _time user src_user TargetUserName EventCode
| eval action=case(EventCode=4720,"User Created", EventCode=4728,"Added to Admin Group")
```

3.3 Suspicious Process Creation (Sysmon)

```
index=sysmon sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
EventCode=1
| search Image="*powershell.exe" OR Image="*cmd.exe" OR Image="*wmic.exe"
| table _time Computer User Image CommandLine ParentImage
```

3.4 Unusual PowerShell Execution

```
index=sysmon EventCode=1 Image="*powershell.exe"
| stats count by CommandLine
| where count > 10
| sort - count
```

3.5 Detect Base64-Encoded PowerShell Commands

```
index=sysmon EventCode=1 Image="*powershell.exe"
| regex CommandLine="(?i)base64"
| table _time User Image CommandLine
```

🕵️ 4. Network Threat Hunting

4.1 Suspicious DNS Queries (C2 Detection)

```
index=dns OR index=network sourcetype=dns
| stats count by query
```

| where like(query, "%.cn") OR like(query, "%.ru") OR like(query, "%.top")

| sort - count

4.2 Beaconing Behavior (Consistent Time Intervals)

index=proxy OR index=firewall

| stats earliest(_time) as first latest(_time) as last count by src_ip dest_ip

| eval duration=last-first, interval=duration/count

| where interval < 60

| sort - interval

💀 5. Post-Exploitation and Lateral Movement

5.1 Remote Execution (WMI, PsExec, RDP)

index=wineventlog EventCode=7045 OR EventCode=4624 OR EventCode=4688

| search CommandLine="*psexec*" OR CommandLine="*wmic*" OR LogonType=10

| table _time Computer User CommandLine LogonType

5.2 Registry Persistence

index=sysmon EventCode=13

| search TargetObject="*\\Run*" OR TargetObject="*\\RunOnce*"

| table _time User TargetObject Details

📡 6. Data Exfiltration Detection

6.1 Large Outbound Traffic to Unknown Domains

index=proxy OR index=firewall

| stats sum(bytes_out) as total_out by src_ip dest_domain

| where total_out > 100000000

| sort - total_out

6.2 Suspicious File Uploads

index=proxy OR index=web

| search method=POST OR upload

| stats count by src_ip dest_domain uri

| sort - count

🔐 7. Advanced Analytics (Using Correlation)

Detect Lateral Movement + Privilege Escalation Combined

(index=wineventlog EventCode=4624 LogonType=10)

OR (index=wineventlog EventCode=4728)

| transaction user maxspan=30m

| search eventcount>1

| table _time user src_ip EventCode

🧩 8. Threat Hunting Dashboards (Optional)

You can create **custom dashboards** in Splunk:

- **Panel 1:** Failed Logins Heatmap
- **Panel 2:** Top PowerShell Commands
- **Panel 3:** Beaconing Pattern Graph
- **Panel 4:** Data Exfiltration Volume (bytes_out trend)

Use:

index=* | timechart count by EventCode

🧠 9. MITRE ATT&CK Technique Examples

Tactic	Technique	Splunk Query Example
Persistence	T1547	index=sysmon EventCode=13 TargetObject="*Run*"
Lateral Movement	T1021	index=wineventlog EventCode=4624 LogonType=10

Tactic	Technique	Splunk Query Example
Defense Evasion	T1086	index=sysmon CommandLine="*bypass*"
Exfiltration	T1048	index=proxy bytes_out>100000000

🚀 10. Summary

Goal	Example Query
Detect brute force	EventCode=4625
Detect PowerShell abuse	Image="*powershell.exe" CommandLine="*base64*"
Detect beaconing	stats avg(_time) by dest_ip
Detect data theft	bytes_out > 100MB
Detect persistence	TargetObject="*Run*" EventCode=13