Scripts (Hands-On Configs & Commands)

Filebeat Configuration (filebeat.yml):

`yaml

```
filebeat.inputs:
- type: log
  paths:
    - /var/log/auth.log
    - /var/log/apache2/access.log
    - /var/log/apache2/error.log

output.logstash:
  hosts: ["localhost:5044"]
```

Logstash Pipeline (logstash.conf):

`conf

```
input {
  beats {
    port => 5044
  }
}
filter {
  grok {
    match => { "message" => "%{IPORHOST:client} %{USER:authuser}
%{HTTPDATE:timestamp} %{WORD:method} %{URIPATH:request}
%{NUMBER:status}" }
  }
}
output {
  elasticsearch {
```

```
    hosts => ["localhost:9200"]
    index => "siem-logs-%{+YYYY.MM.dd}"
  }
}
```

Attack Simulation Commands:

Simulate failed SSH logins

ssh testuser@localhost

Enter wrong password multiple times

Simulate Apache errors

curl http://localhost/nonexistentpage

Incident Response:

Block suspicious IP

sudo iptables -A INPUT -s <malicious_ip> -j DROP

Notes (Documentation & Observations)

- Filebeat forwards raw logs from system and Apache into Logstash.
- Logstash parses logs using Grok filters to extract IP, timestamp, method, and status codes.
- Elasticsearch indexes logs for search and correlation.
- Kibana visualizes events in dashboards (failed logins, HTTP errors, sudo usage).
- Screenshots should be inserted to show dashboards for:
  - Failed SSH login attempts
  - Apache error codes (404, 500)
  - Sudo usage events

- Attack Simulation:
  - Multiple failed SSH logins → detected as brute force.
  - Apache misconfigurations → detected via error logs.
- Incident Response:
  - Suspicious IPs blocked.
  - Accounts reviewed for privilege escalation.
  - Timeline reconstructed in Kibana.

Methodologies (Structured Approach)

1. Planning
- Objective: Build a mini SIEM using ELK Stack for anomaly detection.
- Scope: Authentication logs, Apache logs, system events.
- Tools: Elasticsearch, Logstash, Kibana, Filebeat.

2. Log Collection
- Configure Filebeat to collect logs from /var/log/auth.log and Apache logs.
- Forward logs to Logstash for parsing.

3. Parsing & Indexing
- Apply Grok filters to extract structured fields.
- Store logs in Elasticsearch with daily indices.

4. Visualization
- Create Kibana dashboards for:
  - Failed login attempts per IP
  - HTTP status trends
  - Privilege escalation events

5. Attack Simulation

- Generate failed SSH logins.
- Trigger Apache errors.
- Observe anomalies in Kibana dashboards.

6. Detection & Response

- Alerts triggered when thresholds exceeded.
- Containment via firewall rules and account lockout.
- Incident timeline reconstructed in Kibana.

7. Mitigation

- Harden SSH with fail2ban.
- Secure Apache with headers.
- Automate alerts with Watcher/ElastAlert.
- Regularly update detection rules.