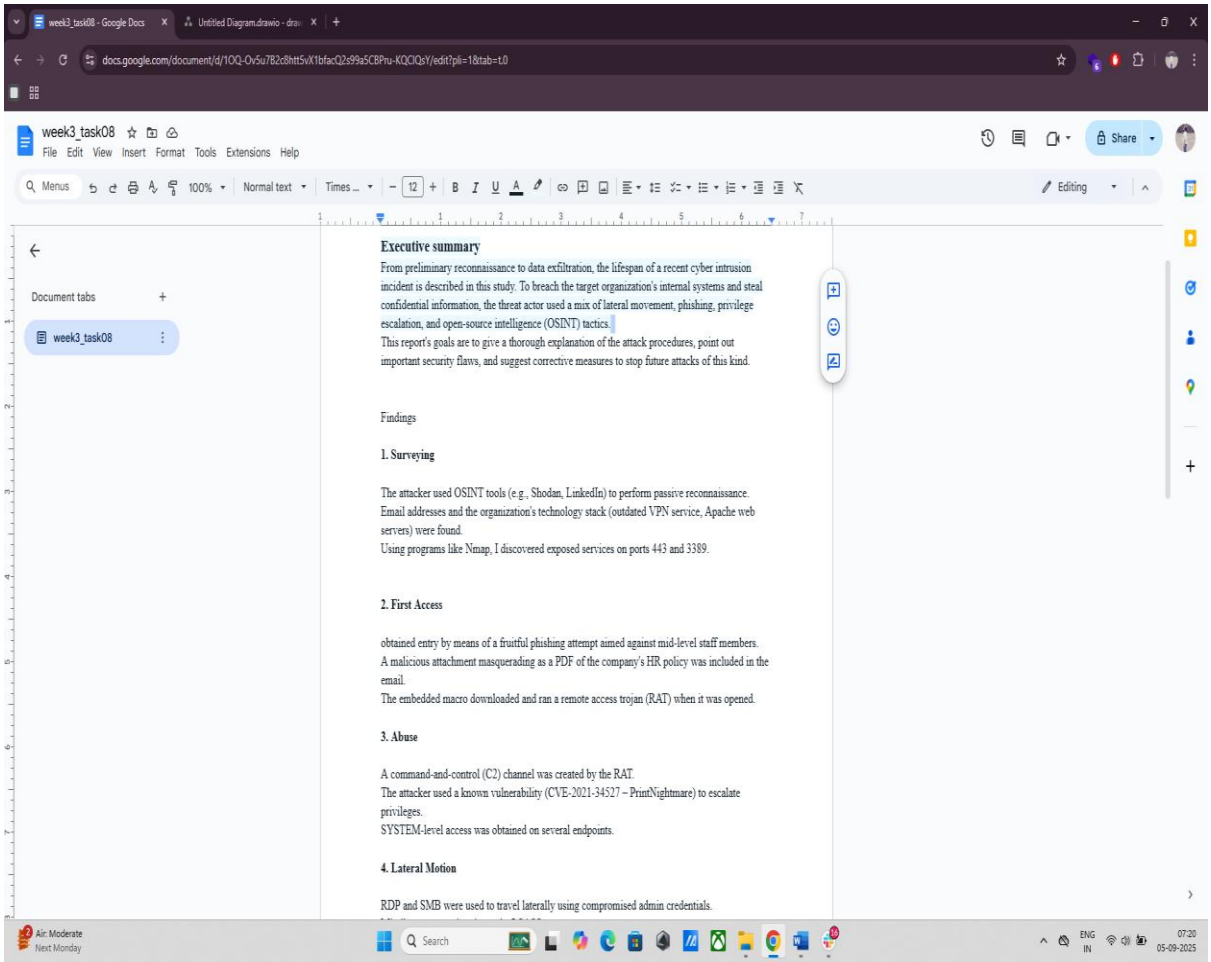
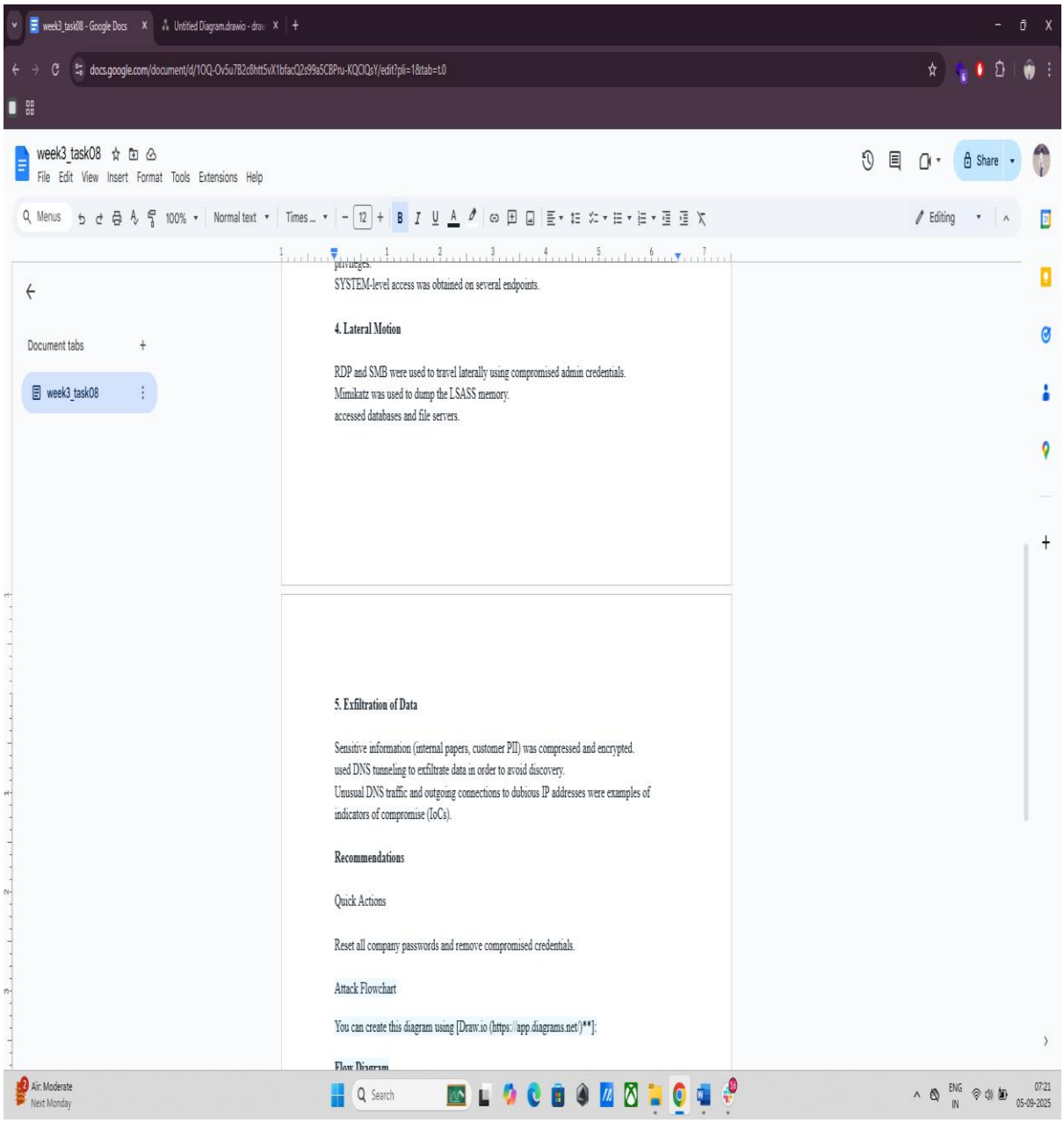
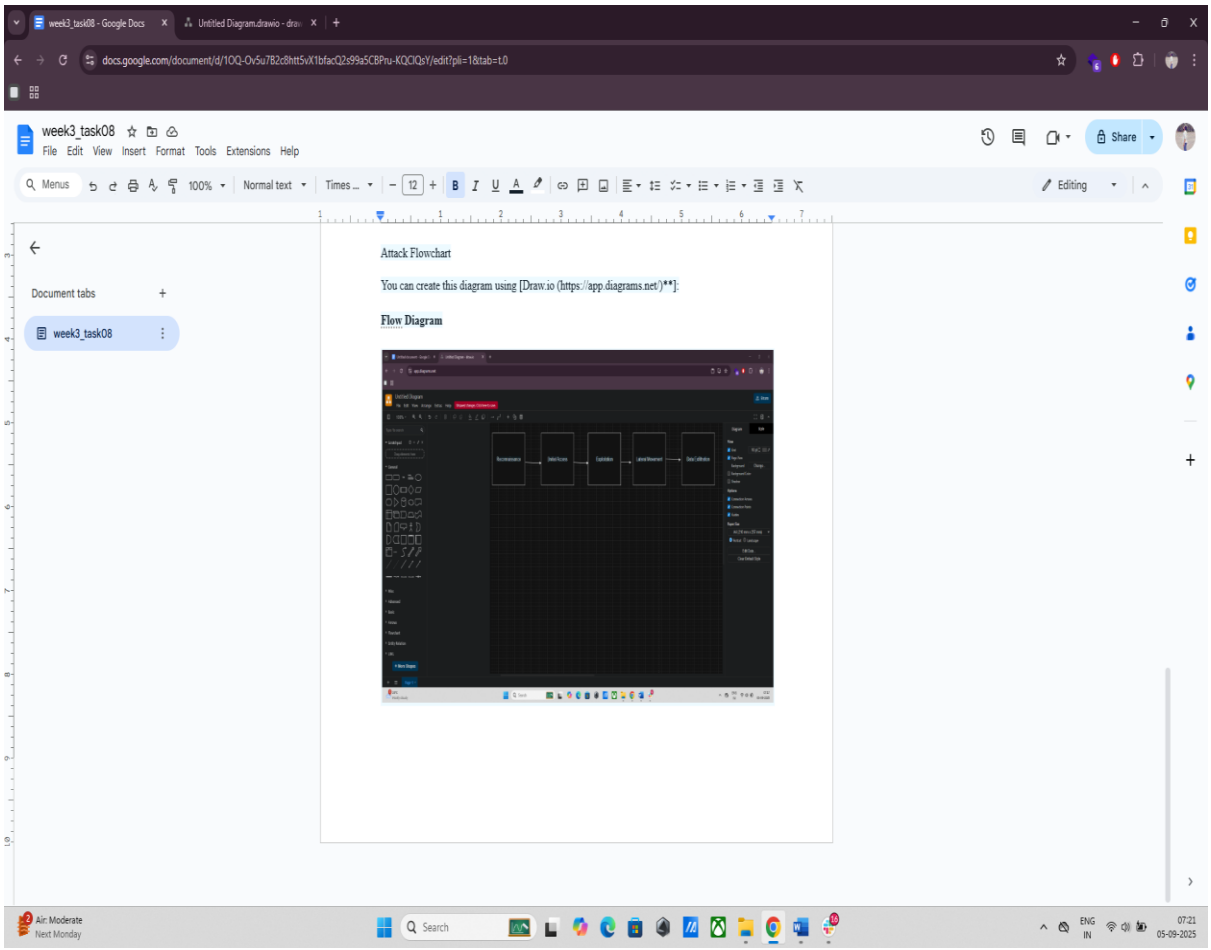
8. Red Team Report Creation

Activities:

- **Tools:** Google Docs, Draw.io.
- **Tasks:** Document a simulated engagement.
- **Brief:**
- **Report Draft:** Write report (recon to exfil) in Google Docs:
    - Executive Summary
    - Findings
    - Recommendations
    - Attack Flowchart: Diagram with Draw.io (Recon → Initial Access → Exploitation → Lateral Movement).




week3_task08 - Google Docs
Untitled Diagram.drawio - draw
docs.google.com/document/d/1OQ-Ov5u7B2c8htt5vX1bfacQ2s99a5CBPru-KQCIQsY/edit?pli=1&tab=t.0
week3_task08
File Edit View Insert Format Tools Extensions Help
Share
Menus
100%
Normal text
Times ...
12
Editing
Document tabs
week3_task08
privileges.
SYSTEM-level access was obtained on several endpoints.
4. Lateral Motion
RDP and SMB were used to travel laterally using compromised admin credentials.
Mimikatz was used to dump the LSASS memory.
accessed databases and file servers.
5. Exfiltration of Data
Sensitive information (internal papers, customer PII) was compressed and encrypted.
used DNS tunneling to exfiltrate data in order to avoid discovery.
Unusual DNS traffic and outgoing connections to dubious IP addresses were examples of
indicators of compromise (IoCs).
Recommendations
Quick Actions
Reset all company passwords and remove compromised credentials.
Attack Flowchart
You can create this diagram using [Draw.io (https://app.diagrams.net/)**]:
Flow Diagram
Air: Moderate
Next Monday
Search
ENG
IN
07:21
05-09-2025


week3_task08 - Google Docs
Untitled Diagram.drawio - draw
docs.google.com/document/d/1OQ-Ov5u7B2c8htt5vX1bfacQ2s99a5CBPru-KQCIQsY/edit?pli=1&tab=t.0
week3_task08
File Edit View Insert Format Tools Extensions Help
Share
Menus
Normal text
Times ...
Editing
Document tabs
week3_task08
Attack Flowchart
You can create this diagram using [Draw.io (https://app.diagrams.net/)**].
Flow Diagram
Air: Moderate
Next Monday
Search
ENG
IN
07:21
05-09-2025