7. Post-Exploitation and Exfiltration

Activities:

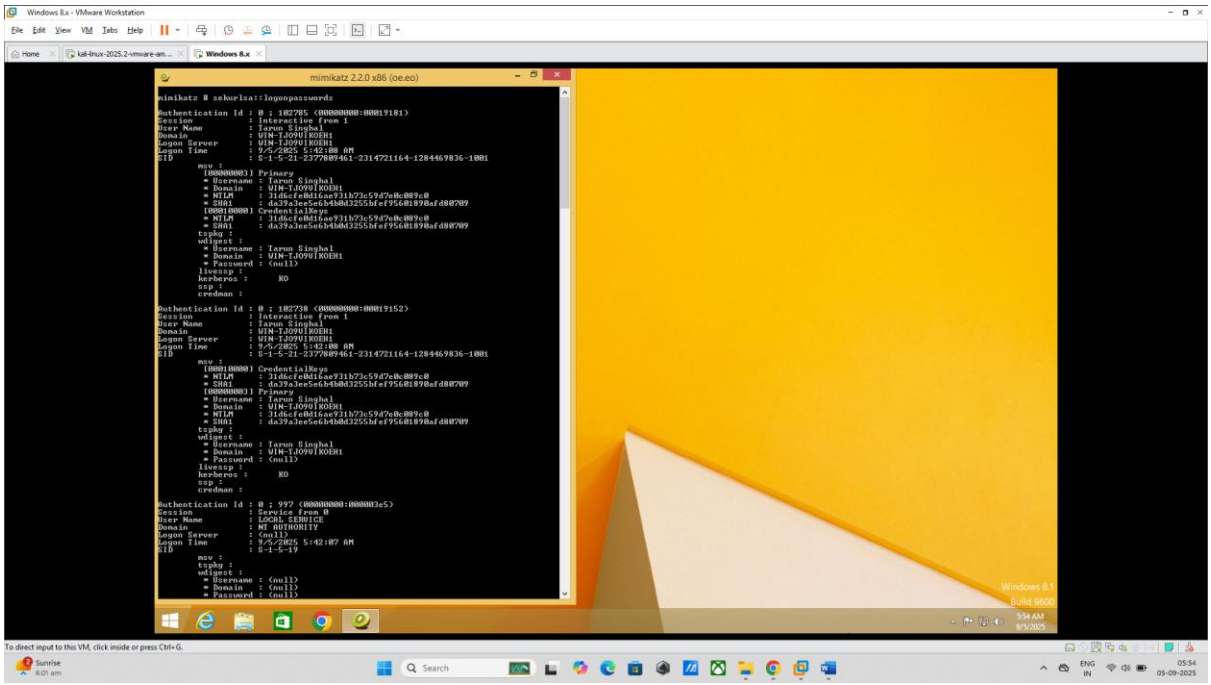
- **Tools:** Mimikatz, Exfiltool.
- **Tasks:** Dump credentials, exfiltrate data.
- **Brief:**

Credential Dump: Run Mimikatz in a Windows VM to extract hashes. Log:

| Hash Type | Username | Hash Valu|

|----------|---------------|------------------|

| NTLM | Administrator | aad3b435b514... |



- Exfiltration: Use DNS tunneling for mock data: verify.