Windows Passwörter

Es gibt zwei Hash-Algorithmen unter Windows: das veraltete LM und das neuere NTLM bzw. NTLMv2. Da LM die Sicherheit eines Systems aushebeln kann, sollte es unbedingt deaktiviert werden. Hierfür muss folgender Registry Schlüssel erzeugt werden:

```
HKLM\System\CurrentControlSet\Control\LSA
NoLMHash  REG_DRWORD  1
```

Die Passwörter werden in der SAM Datenbank gespeichert. Diese ist im laufenden System nicht lesbar, man muss also offline auf die Platte zugreifen oder die Werte aus dem RAM auslesen. Letzteres macht beispielsweise PGDump.