

Challenge
312 Solves

# Preferential Treatment

## 150

We have an old Windows Server 2008 instance that we lost the password for. Can you see if you can find one in this packet capture?

gpnightma...

Flag
Submit

Follow tcp stream and find cpassword

```

.....SMB.....
.....};;.....}.<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EC16-4b4c-9934-544FC6D24D26}">
  <User clsid="{DF5F1855-52E5-4d24-881A-D9BDE98BA1D1}" name="swampctf.com\Administrator" image="2"
    changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}">
    <Properties action="U" newName="" fullName="" description=""
      cpassword="dAw7VQvfj9rs53A8t4PudTVf85Ca5cmC1Xjx6TpI/cS8wD4D8DXbKiWIZslihdJw3Rf+ijboX7FgLW7pF0K6x7dfhQ8gxLq34ENGjN8eTOI="
      changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="swampctf.com\Administrator"/>
  </User>
</Groups>

```

The challenge mention about older windows server 2008. So to decrypt this password im using gpp-decrypt

```

$ (zeqzoqⓈ zeqzoq)-[~]
$ gpp-decrypt dAw7VQvfj9rs53A8t4PudTVf85Ca5cmC1Xjx6TpI/cS8wD4D8DXbKiWIZslihdJw3Rf+ijboX7FgLW7pF0K6x7dfhQ8gxLq34ENGjN8eTOI=
swampCTF{4v3r463_w1nd0w5_53cur17y}

```

Flag: swampCTF{4v3r463\_w1nd0w5\_53cur17y}