

## CPR E 2300 HW 2

Lachlan Kreunen

[kreunen@iastate.edu](mailto:kreunen@iastate.edu)

a. Determine the used hash type of the password.

The shadow file line is:

```
admin1:$6$xcgLS35S6$2UjEq.dUhICPw9zgDVJXcQYQp/9ilLPQt/8Zgu0uwngl5mVvB1eKQ
G9SnVLjmOOfkB4Jjb5VSAXGXjY4Cf5k90:18169:0:99999:7:::
```

The line starts with “\$6\$” which indicates that the password is hashed with the SHA-512 hashing algorithm

b. Determine the salt value of the password.

In the shadow file line, the next segment is the salt string which would be “xcgLS35S6”

c. Crack the password of the server using OpenSSL tool.

Since I went the route of using passLib and python:

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lachl>pip install passlib
Collecting passlib
  Downloading passlib-1.7.4-py2.py3-none-any.whl.metadata (1.7 kB)
  Downloading passlib-1.7.4-py2.py3-none-any.whl (525 kB)
    525.6/525.6 kB 6.6 MB/s eta 0:00:00
Installing collected packages: passlib
Successfully installed passlib-1.7.4

[notice] A new release of pip is available: 24.3.1 -> 25.0.1
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\lachl>python.exe -m pip install --upgrade pip
Requirement already satisfied: pip in c:\users\lachl\appdata\local\programs\python\python313\lib\site-packages (24.3.1)
Collecting pip
  Downloading pip-25.0.1-py3-none-any.whl.metadata (3.7 kB)
  Downloading pip-25.0.1-py3-none-any.whl (1.8 MB)
    1.8/1.8 MB 10.0 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 24.3.1
    Uninstalling pip-24.3.1:
      Successfully uninstalled pip-24.3.1
  Successfully installed pip-25.0.1
```

But checked in openssl that the hash is still the same:

```
C:\Users\lachl>openssl passwd -6 -salt xcgLS35S6 P@ssw0rd
$6$xcgLS35S6$2UjEq.dUhICPw9zgDVJXcQYQp/9ilLPQt/8Zgu0uwngl5mVvB1eKQG9SnVLjmOOfkB4Jjb5VSAXGXjY4Cf5k90
```

d. Submit commented, working, and compiled code/script that cracks the password

Done

e. Provide the password

**Password found: P@ssw0rd**

```
PS C:\Users\lachl\desktop\Hw2> ls

Directory: C:\Users\lachl\desktop\Hw2

Mode                LastWriteTime         Length Name
----                -
-a----            2/19/2025   8:23 PM          1148 passwordCrack.py
-a----            2/19/2025   8:22 PM        851085 passwords.txt
-a----            2/19/2025   8:22 PM          125 shadow.txt

PS C:\Users\lachl\desktop\Hw2> python passwordCrack.py
Password found: P@ssw0rd
```