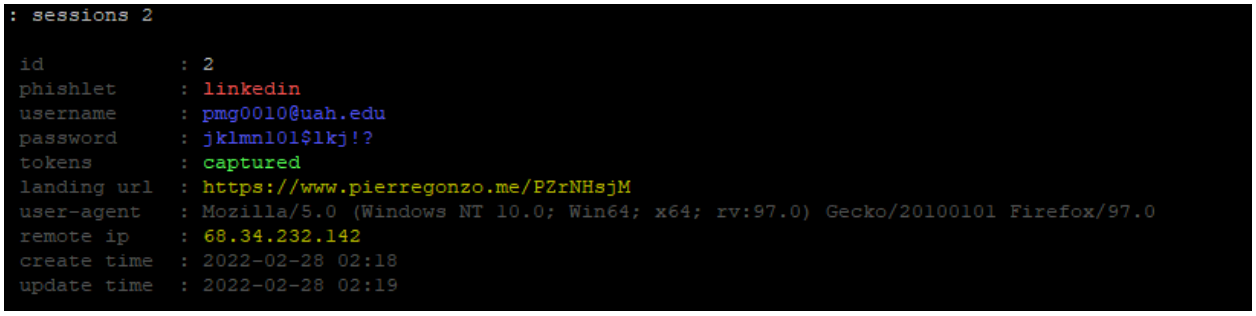
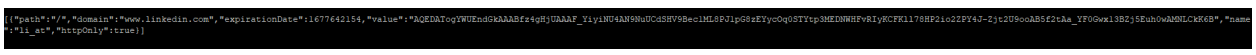
Team:
Bryce Brasfield
Pierre Gonzalez

1.
Below are the screenshots taken from Pierre Gonzalez's VM. We were able to achieve taking the user's username, password, and session cookie (cookie provided in text format), but we were not able to hijack the session through our web browser but every other step in the process was taken care of. We could not find a way to enter the cookie into our browser and sign into the account.

[{"path":"/","domain":"www.linkedin.com","expirationDate":1677642154,"value":"AQEDATogYWUEndGkAAABfz4gHjUAAAF_YiyiNU4AN9NuUCdSHV9Bec1ML8PJ1pG8zEYycOq0STYtp3MEDNWHFvRIyKCFKll78HP2io2ZPY4J-Zjt2U9ooAB5f2tAa_YF0Gwx13BZj5Euh0wAMNLCkK6B","name":"li_at","httpOnly":true}]

[{"path":"/","domain":"www.linkedin.com","expirationDate":1677550782,"value":"AQEDATogYWUEndGkAAABfz4gHjUAAAF_YiyiNU4AN9NuUCdSHV9Bec1ML8PJ1pG8zEYycOq0STYtp3MEDNWHFvRIyKCFKll78HP2io2ZPY4J-Zjt2U9ooAB5f2tAa_YF0Gwx13BZj5Euh0wAMNLCkK6B","name":"li_at","httpOnly":true}]

2.
a) Password465 - jtr could not brute force this password. Ran several hours and it still hadn't reached a password with a capital letter as the first character. A Dictionary attack with rockyou.txt failed as well, unless "Password465" was specifically added in. Adding "Password465" into rockyou.txt broke the password in a matter of seconds. A custom wordlist

with custom rules (for example a combination of “password” in varying degrees of capitals plus numbers) could possibly brute force this in a reasonable amount of time.
(b) Ball2022Game - again jtr could not brute force this password (this will be the case for all of these). Again, a dictionary attack with rockyou.txt also failed (this will also be the case for all of these). Finally once the specific password was added to a custom wordlist, it was cracked in seconds.
(c) SuperBowl!Hooray
(d) E$%!&dret5@!#@$@$
(e) !123#UAH$Go

- The rest of these are the same. Unless a password is well known or extremely simple (short with only lower case letters) it will likely not be cracked.

3.
The script we used is below:

```
#!/bin/bash

numPasswords=$(cat rockyou.txt | wc -l)

echo "There are $numPasswords passwords in rockyou.txt"

pWordsWithPassword=$(cat rockyou.txt | grep -i "password" | wc -l)

echo "$pWordsWithPassword of them contain 'password'"

numSpecial=$(cat rockyou.txt | grep -a [0-9] | grep -a [A-Za-z] | grep -a [\!\@\#\$\%\&] | wc -l)

echo "$numSpecial of them contain at least one letter, one number, and one special character"
```

The output of it is:

```
There are 14344391 passwords in rockyou.txt
4690 of them contain 'password'
159294 of them contain at least one letter, one number, and one special character
```

Output explanation
Meaning there are 14344391 passwords in the file
4690 passwords contain any variant of the word “password”
And 159294 passwords contain one letter, number, and special character