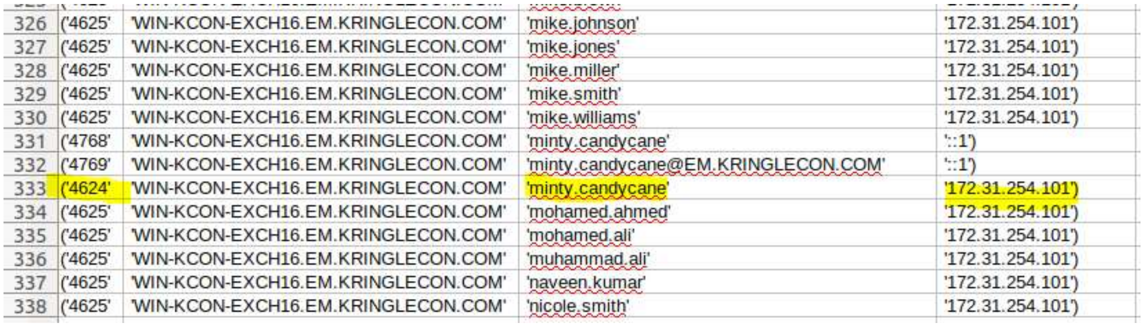
Terminal--Yule Log (part 4)

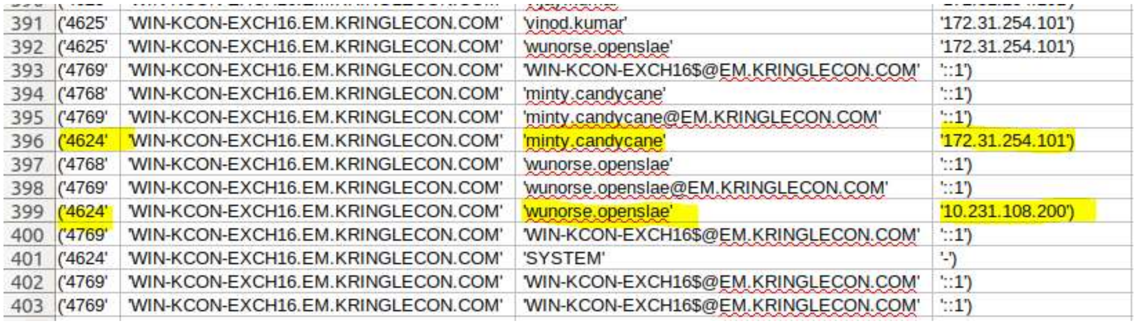
Solution

When the results of our Python script and grep commands are open in a spreadsheet, we see a long series of failed login attempts (4625) all from IP address 172.31.254.101, and the user names are in alphabetical order (that's helpful for us.) In between mike.williams and mohammed.ahmed, we see a successful login from the attacker's address, 172.31.254.101.



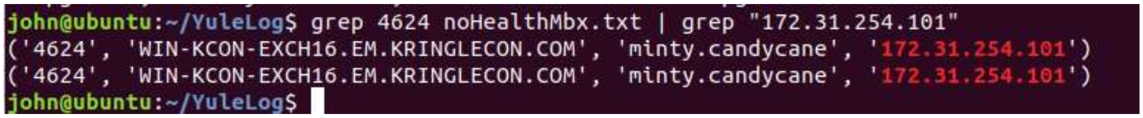
326	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mike.johnson'	'172.31.254.101')
327	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mike.jones'	'172.31.254.101')
328	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mike.miller'	'172.31.254.101')
329	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mike.smith'	'172.31.254.101')
330	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mike.williams'	'172.31.254.101')
331	('4768'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'minty.candycane'	'::1')
332	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'minty.candycane@EM.KRINGLECON.COM'	'::1')
333	('4624'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'minty.candycane'	'172.31.254.101')
334	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mohamed.ahmed'	'172.31.254.101')
335	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'mohamed.ali'	'172.31.254.101')
336	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'muhammad.ali'	'172.31.254.101')
337	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'naveen.kumar'	'172.31.254.101')
338	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'nicole.smith'	'172.31.254.101')

At the end of the file we see a second login to Minty's account from the attacker's IP address. Notice that Wunorse logs in just after that, but with an IP address of 10.231.108.200. Scanning through the file shows us most successful logins, that appear to be normal logins, come from IP addresses in that same range.



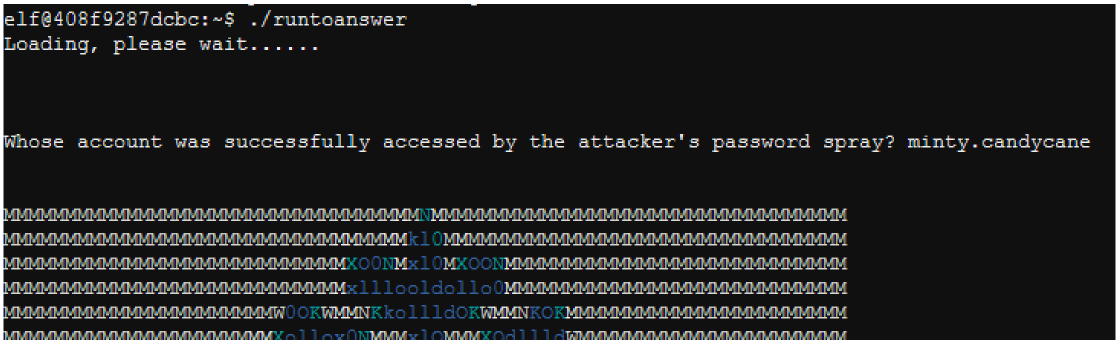
391	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'vinod.kumar'	'172.31.254.101')
392	('4625'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'wunorse.openslae'	'172.31.254.101')
393	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'WIN-KCON-EXCH16$@EM.KRINGLECON.COM'	'::1')
394	('4768'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'minty.candycane'	'::1')
395	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'minty.candycane@EM.KRINGLECON.COM'	'::1')
396	('4624'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'minty.candycane'	'172.31.254.101')
397	('4768'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'wunorse.openslae'	'::1')
398	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'wunorse.openslae@EM.KRINGLECON.COM'	'::1')
399	('4624'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'wunorse.openslae'	'10.231.108.200')
400	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'WIN-KCON-EXCH16$@EM.KRINGLECON.COM'	'::1')
401	('4624'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'SYSTEM'	'-')
402	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'WIN-KCON-EXCH16$@EM.KRINGLECON.COM'	'::1')
403	('4769'	'WIN-KCON-EXCH16.EM.KRINGLECON.COM'	'WIN-KCON-EXCH16$@EM.KRINGLECON.COM'	'::1')

As a test, let's search the file for other successful logins from the 172.31.254.101 address.



```
john@ubuntu:~/YuleLog$ grep 4624 noHealthMbx.txt | grep "172.31.254.101"
('4624', 'WIN-KCON-EXCH16.EM.KRINGLECON.COM', 'minty.candycane', '172.31.254.101')
('4624', 'WIN-KCON-EXCH16.EM.KRINGLECON.COM', 'minty.candycane', '172.31.254.101')
john@ubuntu:~/YuleLog$
```

It appears Minty was the only one they caught.

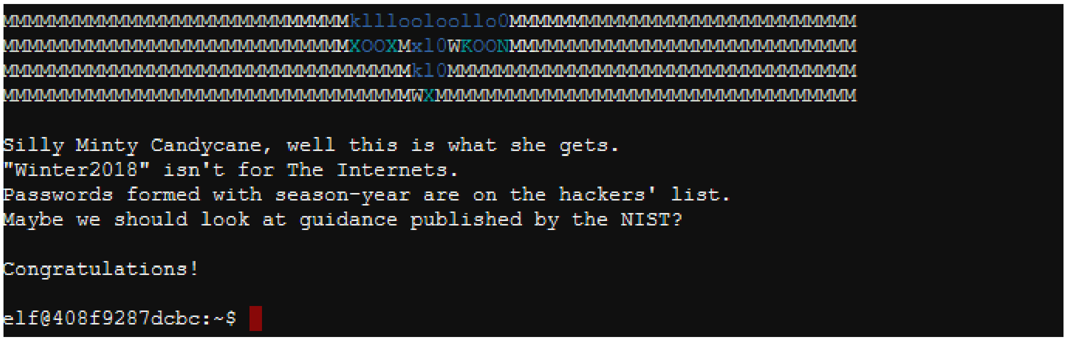


```
elf@408f9287dcbc:~$ ./runtoanswer
Loading, please wait......



Whose account was successfully accessed by the attacker's password spray? minty.candycane


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMkl0MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMXO0NMxl0MXOONMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMxlllooldollo0MMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMW0OKWMMNKkollldOKWMMNKOKMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMXollox0NMMMxl0MMMXOdllldWMMMMMMMMMMMMMMMMMMMMMM
```



```
MMMMMMMMMMMMMMMMMMMMMMMMMMMMklllooloollo0MMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMXOOXMxl0WKOONMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMkl0MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWXMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM

Silly Minty Candycane, well this is what she gets.
"Winter2018" isn't for The Internets.
Passwords formed with season-year are on the hackers' list.
Maybe we should look at guidance published by the NIST?

Congratulations!

elf@408f9287dcbc:~$ 
```

Hand In

1) What makes a password spraying attack more likely to be successful that a brute force attack?

2) Why are password spraying attacks more difficult to detect?

Up Next

Now that we have helped Pepper, we can talk to her to collect our hints and move on to the badge manipulation challenge. Warning: The degree of difficulty increases markedly after this.