ATTACKING PASSWORDS

Deliverable for this lab: briefly add the following information to the deliverable

- ***1.1: the three plaintext passwords and a screenshot of the hashcat terminal window***
- ***1.2: the plain-text password***
- ***1.3: short explanation what the code does***
- ***1.4: a screenshot of Burp Suite running the brute force attack and the password of the compromised account***

1.1 Offline bruteforcing

Scan through the following article: https://www.bleepingcomputer.com/news/security/popular-stock-photo-service-hit-by-data-breach-83m-records-for-sale/ .

The following is an extract of the "123rf.com member.sql" file that was put online by the hackers responsible for the 123RF breach (all personal data is removed and replaced by ***XXXX***):

INSERT INTO `member` (`uid`, `password`, `md5password`, `company`, `first_name`, `last_name`, `street1`, `street2`, `city`, `state`, `country`, `postcode`, `phone`, `email`, `newsletter`, `discount_cur`, `discount_amt`, `source`, `othersource`, `payby`, `paypal_email`, `paymentlimit`, `approved`, `date_register`, `business_name`, `website`, `job`, `showlocation`, `hidephoto`, `agreement`, `reviewnotify`, `referrer`, `allowextended`, `ipaddress`, `am`, `mini_lb`, `firstlogin`, `remark`, `smuser`, `ip_country`, `ip_state`, `allow_ed_move`, `google_email`, `facebook_email`, `google_id`, `facebook_id`, `mem_deactivated`, `external_invite`) VALUES ('smarshall31','','7cf251e1c307449c2bb86aae80803a09','','Shalita','M***XXXX***all','','','','KY','US','','5023378829','**sh*XXX XXXX***@gmail.com','Y','',0.00,0,'','','','N','2016-03-19 00:00:00','','','','','','','','','74.136.***XXX.XXX***','',1,0,'',0,'US','KY','','','','','',0,0),('christine***XXX***','','c931f87b0df0f9186a1ac36f27e11847','','Christine','S***XXX***','***XXX*** Best Road','','Seven Hills','NSW','AU','2147','02 9621 5518','cm.***XXX***@rocketmail.com','Y','',0.00,7,'','','','50.00','N','2012-06-25 00:00:00','','','','','','','Y','','Y','110.142.***XXX.XXX***','',1,1,'',0,'AU','','','','','','',0,0),('brabecova','','da03eb30a91ca69c5b3fc804ab78c1d7','','Julia','Br***XXX***','PO Box ***XXX***','','Franconia','NH','US','03580','9176044287','brabe***XXX***@gmail.com','Y','',0.00,0,'','','','','N','2020-03-09 11:08:35','','','','','','','','','','72.169.80.71','',1,0,'',0,'US','','','','','','',0,0)

Use hashcat to break the hashes and find the 3 plain-text passwords.

HINT: The hash starting with 'da03…' is the representation of an 8-character password

HINT 2: *Hashcat (https://hashcat.net/hashcat/) is a tool that is often used to crack this kind of passwords. Check for examples at https://www.incredigeek.com/home/hashcat-examples/ and consult https://hashcat.net/wiki/doku.php?id=example_hashes for the kind of hashes that can be cracked by Hashcat.*

HINT 3: An example command is the following:

hashcat -m 0 -a 3 098f6bcd4621d373cade4e832627b4f6 --increment -1 ?l?u?d?s ?1?1?1?1 -O

-m 0: mode 0 => see https://hashcat.net/wiki/doku.php?id=example_hashes
-a 3: this is the attack mode. "3" tells us it is a bruteforce attack. Alternatively you could use "0" for a dictionary attack
098f6bcd4621d373cade4e832627b4f6: the hash we want to crack
--increment: try everything from 1 character up to the amount of characters specified (see next)
-1 ?l?u?d?s: we configure '?1' as a placeholder for a l=lowercase, u=uppercase, d=digit, or s=symbol character
?1?1?1?1: we tell hashcat to try 4-character passwords. Since we are using '?1' as a placeholder, the password can consist of lowercase, uppercase, digits, and symbols

1.2 Offline bruteforcing – slow hashes

Scan through the following article: https://www.bleepingcomputer.com/news/security/hacker-leaks-full-database-of-77-million-nitro-pdf-user-records/

The following is an extract of the "nitrocloud.tsv" file that was put online by the hackers responsible for the Nitro breach (all personal data is removed and replaced by ***XXXX***):

COPY users.user_credential (id, tmp_admin, agreed, created, email, firstname, lastname, password, passwordreset, verified, avatar, settings, source, notifications, status, secret, confirmed_client_access, account_id, timezone, dateformat, verify_remind, desktop_version, locale, prompts, title, company, sem_id, updated_at, tos_pp_accepted_at, remote_ip) FROM stdin;

96344794594287225 f t 2013-11-07 02:14:40.956 f***XXXX***4@gmail.com christine $2a$10$..Iezqezu.68Vr10nO708.gVqv0RbiPLa1ReuzQ56VKtjoO8WcLk2 \N t null|null 4 pdftoword 0 ACTIVE HWJbk99Wwk58F2pOwNZ1380525358355GFxzg9AFjtZcYHWDm t 5115647933114204320 Africa/Casablanca \N \N \N \N 0 \N \N 96344794594287225 \N \N \N

Can you find the plain-text password?

1.3 HIBP

The HIBP API (https://haveibeenpwned.com/API/v3) can be used to check that a password is not yet present in a breach list. Through this exercise you will try out that API.

Run the following code on runkit.com:

```
const hibp = require('hibp');

const suffix = '1E4C9B93F3F0682250B6CF8331B7EE68FD8';
hibp.pwnedPasswordRange('5BAA6')
  // filter to matching suffix
  .then(results => results.filter(row => row.suffix === suffix))
  // return count if match, 0 if not
  .then(results => (results[0] ? results[0].count : 0))
  .catch(err => {
    // ...
  });
```

Look at the output. What does it do?

1.4 Online bruteforcing

Execute an online bruteforcing attack against the following user: ‘admin@juice-sh.op’. Use Burp Suite. Find out how to do that using the Portswigger Academy website… or use Youtube.