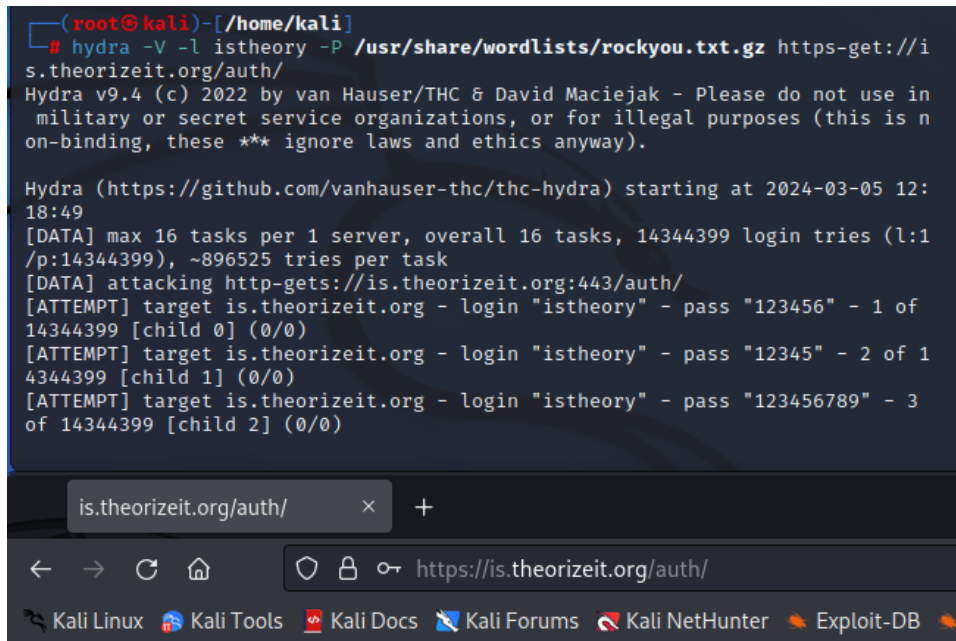


Part 1



The screenshot shows a terminal window on a Kali Linux machine. The user runs the command `hydra -V -l istheory -P /usr/share/wordlists/rockyou.txt.gz https-get://is.theorizeit.org/auth/`. The terminal output shows Hydra v9.4 starting at 2024-03-05 12:18:49, attacking the target `https://is.theorizeit.org:443/auth/` with the username `istheory`. It shows three password attempts: `"123456"`, `"12345"`, and `"123456789"`, all of which failed. Below the terminal, a web browser window is open to `is.theorizeit.org/auth/`, displaying the message "Hello, world!".

```
(root@kali)-[/home/kali]
# hydra -V -l istheory -P /usr/share/wordlists/rockyou.txt.gz https-get://is.theorizeit.org/auth/
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-05 12:
18:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking http-gets://is.theorizeit.org:443/auth/
[ATTEMPT] target is.theorizeit.org - login "istheory" - pass "123456" - 1 of
14344399 [child 0] (0/0)
[ATTEMPT] target is.theorizeit.org - login "istheory" - pass "12345" - 2 of 1
4344399 [child 1] (0/0)
[ATTEMPT] target is.theorizeit.org - login "istheory" - pass "123456789" - 3
of 14344399 [child 2] (0/0)
```

is.theorizeit.org/auth/ x +

← → ↻ 🏠 🔒 🔑 https://is.theorizeit.org/auth/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Hello, world!

(Q1) Why is this attack considered an online attack?

This is considered an online attack since we are attempting to gain unauthorized access to <https://is.theorizeit.org/auth/> over a network. We are using Hydra to perform online password brute-force attacks, through online network protocols like HTTP. Due to this, the attack requires internet and we as we are interacting with the web service.

(Q2) What kind of password attack did we do in this task?

We did a dictionary attack as we received a list of leaked passwords to try and get access to the website.

(Q3) List three countermeasures that organizations could implement specifically against online attacks?

Use Strong Passwords and Extra Security Steps: Make sure only the right people can get into your company's online spaces by using strong passwords and extra steps like MFA.

Keep Software Up to Date: Make sure all the computer programs and systems your company uses are the latest version. Updating means you're patching those holes before hackers can sneak through.

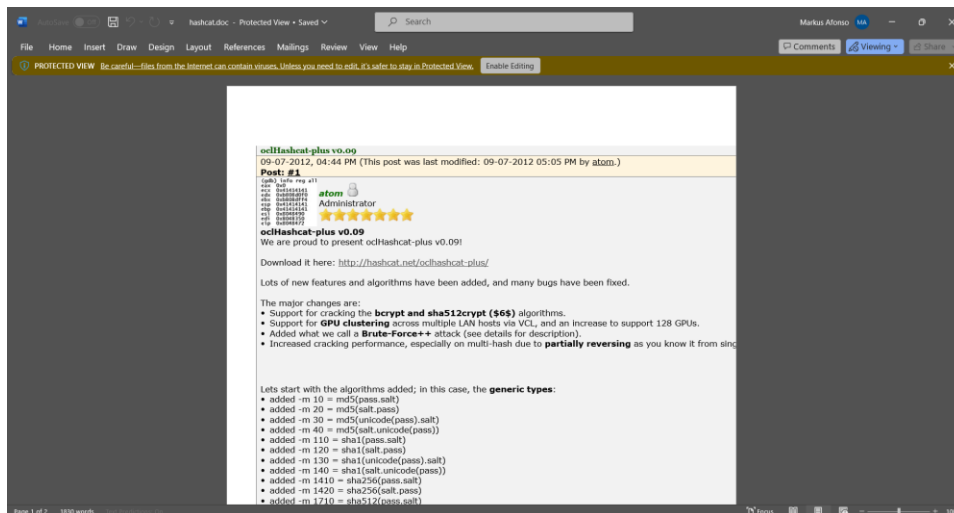
Watch for Threats and Be Ready to Act: Use special tools that can spot when someone is trying to break into your systems and have a plan to stop them.

(Q4) Explain if online attacks are feasible choices for an exhaustive (trying all different combinations) brute-force attack.

Online brute-force attacks, where hackers try every possible password combination, usually don't work well because of a few simple roadblocks. Some examples include websites having rules that stop you from guessing too many times by locking you out, MFAs requiring an additional code, finally the time and effort, especially when the internet itself can slow things down.

(Q5) What is the password for hashcat.doc? (open the output file and look at the end of the hash) o Download the word file on your computer and verify you can see the content.

The password is 'camp'.



(Q6) What kind of password attack did we do in this task?

in this task, we performed a dictionary attack using Hashcat against a password-protected Word doc.

(Q7) How is this offline password attack different from the online hydra attack you attempted earlier?

The offline attack operates locally on a stored hash, whereas the online attack communicates with a live system over the network. In the offline attack, there's no risk of network latency or communication failures affecting the speed of the attack, unlike in the online attack. The offline attack allows for faster guessing of passwords since it's not limited by network constraints or authentication mechanisms.

(Q8) List three countermeasures that organizations could implement specifically against offline attacks.

- Use strong and unique salts: Salting passwords before hashing adds random data to each password, making them unique even if the passwords themselves are the same
- Employ slow hashing algorithms: Using slow hashing algorithms like bcrypt, scrypt, or Argon2

- Implement strong access controls: Limiting access to password hashes and ensuring that only authorized personnel have access to them can prevent attackers from obtaining the hashes needed for offline attacks

(Q9) What's the purpose of -m 100 option in the above command? (Hint: man hashcat)

We specified the specific hash type of SHA1

```
-m, --hash-type=NUM
Hash-type, see references below
```

```
Hash types
0 = MD5
10 = md5($pass.$salt)
20 = md5($salt.$pass)
30 = md5(unicode($pass).$salt)
40 = md5($salt.unicode($pass))
50 = HMAC-MD5 (key = $pass)
60 = HMAC-MD5 (key = $salt)
100 = SHA1
110 = sha1($pass.$salt)
120 = sha1($salt.$pass)
130 = sha1(unicode($pass).$salt)
140 = sha1($salt.unicode($pass))
```

(Q10) What kind of password attack did we do in this task?

A dictionary attack. Hashcat tries each password from a provided wordlist against the hashed passwords to find a match.

(Q11) How many passwords were you able to recover using the Hashcat command above?

We recovered 144,622 passwords.

```
(kali@kali)-[~/lab7]
$ wc -l LinkedIn_cracked.txt
144622 LinkedIn_cracked.txt
```

(Q12) What is the purpose of using rules in this command?

the purpose of using rules in the command is to apply common patterns or transformations to the passwords in the wordlist (rockyou.txt) before attempting to crack the hashes.

(Q13) How many total passwords were you able to recover after using this rulesbased attack in combination with the earlier straight attack?

We recovered 233,812 passwords.

```
(kali@kali)-[~/lab7]
$ wc -l LinkedIn_cracked.txt
233812 LinkedIn_cracked.txt
```

(Q14) What does option -a 6 mean in the above command?

The '-a' specifies attack, but since it's 'a 6' it's an attack combining to methods dictionary attack with a mask attack which is a hybrid attack. This used to create a larger combination of potential passwords.

```
-a, --attack-mode=NUM
    Attack-mode, see references below
```

```
Permutation attack-mode options
Outfile formats
1 = hash[:salt]
2 = plain
3 = hash[:salt]:plain
4 = hex_plain
5 = hash[:salt]:hex_plain
6 = plain:hex_plain
7 = hash[:salt]:plain:hex_plain
8 = crackpos
9 = hash[:salt]:crack_pos
10 = plain:crack_pos
11 = hash[:salt]:plain:crack_pos
12 = hex_plain:crack_pos
13 = hash[:salt]:hex_plain:crack_pos
14 = plain:hex_plain:crack_pos
15 = hash[:salt]:plain:hex_plain:crack_pos
```

(Q15) How many total passwords were you able to recover after using this hybrid attack combined with the earlier straight and rule-based attacks?

We recovered 239,526 passwords.

```
(kali@kali)-[~/lab7]
$ wc -l LinkedIn_cracked.txt
239526 LinkedIn_cracked.txt
```

(Q16) How many total passwords were you able to recover after using this hybrid attack combined with all earlier attacks?

We recovered 256,933 passwords.

```
(kali@kali)-[~/lab7]
$ wc -l LinkedIn_cracked.txt
256933 LinkedIn_cracked.txt
```