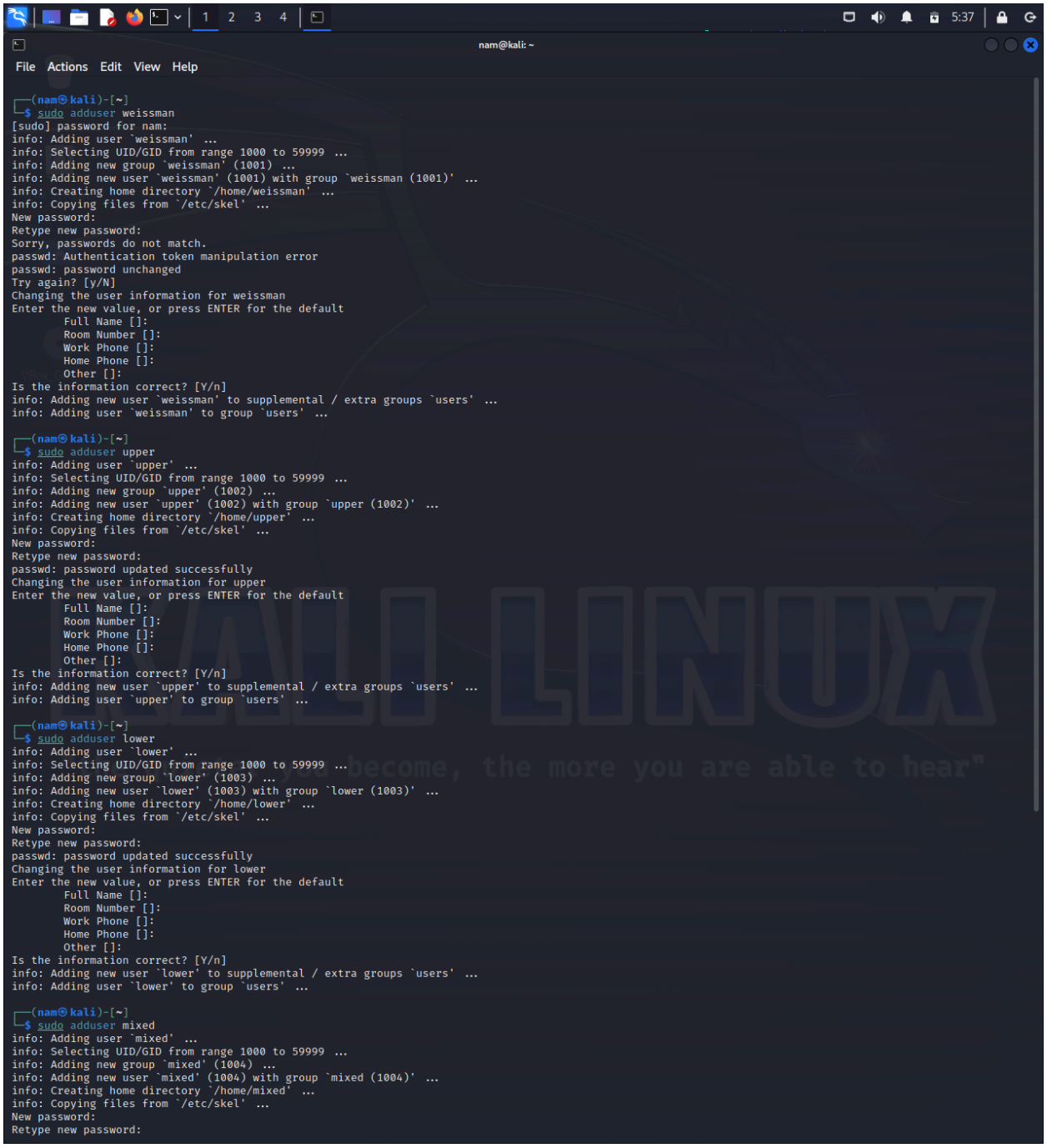
11.01


1 2 3 4
4:52
nam@kali: ~
File Actions Edit View Help
JOHN(8) System Manager's Manual JOHN(8)
NAME
john - a tool to find weak passwords of your users
SYNOPSIS
john [options] password-files
DESCRIPTION
This manual page documents briefly the john command. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. john, better known as John the Ripper, is a tool to find weak passwords of users in a server. John can use a dictionary or some search pattern as well as a password file to check for passwords. John supports different cracking modes and understands many ciphertext formats, like several DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows NT passwords.
USAGE
To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental".
Once John finds a password, it will be printed to the terminal and saved into a file called ~/.john/john.pot. John will read this file when it restarts so it doesn't try to crack already done passwords.
To see the cracked passwords, use
john -show passwd
Important: do this under the same directory where the password was cracked (when using the cronjob, /var/lib/john), otherwise it won't work.
While cracking, you can press any key for status, or Ctrl+C to abort the session, saving point information to a file (~/.john/john.rec by default). By the way, if you press Ctrl+C twice John will abort immediately without saving. The point information is also saved every 10 minutes (configurable in the configuration file, ~/.john/john.ini or ~/.john/john.conf) in case of a crash.
To continue an interrupted session, run:
john -restore
Now, you may notice that many accounts have a disabled shell, you can make John ignore these (assume that shell is called /etc/expired):
john -show -shells:-/etc/expired passwd
You might want to mail all the users who got weak passwords, to tell them to change the passwords. It's not always a good idea though (unfortunately, lots of people seem to ignore such mail, it can be used as a hint for crackers, etc), but anyway, I'll assume you know what you're doing. Get a copy of the 'mailer' script supplied with John, so you won't change anything that's under /usr/sbin ; edit the message it sends, and possibly the mail command inside it (especially if the password file is from a different box than you got John running on). Then run:
./mailer passwd
Anyway, you probably should have a look at /usr/share/doc/john/OPTIONS for a list of all the command line options, and at /usr/share/doc/john/EXAMPLES for more John usage examples with other cracking modes.
OPTIONS
All the options recognized by john start with a single dash ('-'). A summary of options is included below.
-external:MODE
Enables an external mode, using external functions defined in ~/john.ini's [List.External:MODE] section.
-format:NAME
Allows you to override the ciphertext format detection. Currently, valid format names are DES, BSDI, MD5, BF, AFS, LM. You can use this option when cracking or with '-test'. Note that John can't crack password files with different ciphertext formats at the same time.
-groups:[~]GID[,..]
Tells John to load users of the specified group(s) only.
-incremental[:MODE]
Enables the incremental mode, using the specified ~/john.ini definition (section [Incremental:MODE], or [Incremental:All] by default).
-makechars:FILE
Generates a charset file, based on character frequencies from ~/.john/john.pot, for use with the incremental mode. The entire ~/.john/john.pot will be used for the charset file unless you specify some password files. You can also use an external filter() routine with this option.
-restore[:FILE]
Continues an interrupted cracking session, reading point information from the specified file (~/.john/john.rec by default).
-rules Enables wordlist rules, that are read from [List.Rules:Wordlist] in /etc/john/john.conf (or the alternative configuration file you might specify on the command line).
This option requires the -wordlist option to be passed as well.
-salts:[~]COUNT
This feature sometimes allows you to achieve better performance. For example you can crack only some salts using '-salts:2' faster, and then crack the rest using '-salts:-2'. Total cracking time will be about the same, but you will get some passwords cracked earlier.
Manual page john(8) line 1 (press h for help or q to quit)


1 2 3 4
4:53
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo john
[sudo] password for nam:
Created directory: /root/.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 SSE2 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.
(nam㉿kali)-[~]
$ man john
(nam㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"


1 2 3 4
5:34
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo john --test
[sudo] password for nam:
Will run 14 OpenMP threads
Benchmarking: descrypt, traditional crypt(3) [DES 128/128 SSE2]... (14xOMP) DONE
Many salts: 41250K c/s real, 3637K c/s virtual
Only one salt: 34491K c/s real, 2714K c/s virtual
Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 128/128 SSE2]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 725
Warning: "Many salts" test limited: 57/256
Many salts: 100141 c/s real, 11463 c/s virtual
Only one salt: 1146K c/s real, 100471 c/s virtual
Benchmarking: md5crypt, crypt(3) 1 (and variants) [MD5 128/128 SSE2 4×3]... (14xOMP) DONE
Many salts: 324867 c/s real, 29040 c/s virtual
Only one salt: 336000 c/s real, 29459 c/s virtual
Benchmarking: md5crypt-long, crypt(3) 1 (and variants) [MD5 32/64]... (14xOMP) DONE
Raw: 58779 c/s real, 5210 c/s virtual
Benchmarking: bcrypt ("$2a$05", 32 iterations) [Blowfish 32/64 X3]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 32
Raw: 10980 c/s real, 989 c/s virtual
Benchmarking: scrypt (16384, 8, 1) [Salsa20/8 128/128 SSE2]... (14xOMP) DONE
Speed for cost 1 (N) of 16384, cost 2 (r) of 8, cost 3 (p) of 1
Raw: 257 c/s real, 24.3 c/s virtual
Benchmarking: LM [DES 128/128 SSE2]... (14xOMP) DONE
Raw: 110218K c/s real, 9241K c/s virtual
Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE
Short: 771840 c/s real, 771840 c/s virtual
Long: 770688 c/s real, 770688 c/s virtual
Benchmarking: tripcode [DES 128/128 SSE2]... (14xOMP) DONE
Raw: 4207K c/s real, 364723 c/s virtual
Benchmarking: AndroidBackup [PBKDF2-SHA1 128/128 SSE2 4x AES]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 10000
Raw: 3103 c/s real, 330 c/s virtual
Benchmarking: adxcrypt, IBM/Toshiba 4690 [ADXCRYPT 32/64]... (14xOMP) DONE
Raw: 40677K c/s real, 4657K c/s virtual
Benchmarking: agilekeychain, 1Password Agile Keychain [PBKDF2-SHA1 AES 128/128 SSE2 4x]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 1000
Raw: 57730 c/s real, 5123 c/s virtual
Benchmarking: aix-ssha1, AIX LPA {ssha1} [PBKDF2-SHA1 128/128 SSE2 4x]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 64
Many salts: 1039K c/s real, 91694 c/s virtual
Only one salt: 1107K c/s real, 92188 c/s virtual
Benchmarking: aix-ssha256, AIX LPA {ssha256} [PBKDF2-SHA256 128/128 SSE2 4x]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 64
Many salts: 309810 c/s real, 27252 c/s virtual
Only one salt: 534898 c/s real, 44880 c/s virtual
Benchmarking: aix-ssha512, AIX LPA {ssha512} [PBKDF2-SHA512 128/128 SSE2 2x]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 64
Many salts: 164696 c/s real, 13966 c/s virtual
Only one salt: 119745 c/s real, 11091 c/s virtual
Benchmarking: andOTP [SHA256 32/64]... (14xOMP) DONE
Raw: 1850K c/s real, 152161 c/s virtual
Benchmarking: ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 128/128 SSE2 4x]... (14xOMP) DONE
Speed for cost 1 (iteration count) of 10000
Raw: 1783 c/s real, 169 c/s virtual
Benchmarking: argon2 [Blake2 SSE2]... (14xOMP) DONE
Speed for cost 1 (t) of 3, cost 2 (m) of 4096, cost 3 (p) of 1, cost 4 (type [0:Argon2d 1:Argon2i]) of 0 and 1
Raw: 652 c/s real, 66.5 c/s virtual
Benchmarking: as400-des, AS/400 DES [DES 32/64]... DONE
Raw: 296912 c/s real, 25049 c/s virtual
Benchmarking: as400-ssha1, AS400-SaltedSHA1 [sha1(utf16be(space_pad_10(uc($s)).$p)) (IBM AS/400 SHA1) 128/128 SSE2 4×1]... DONE
Many salts: 23447K c/s real, 23532K c/s virtual


1 2 3 4
5:37
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo adduser weissman
[sudo] password for nam:
info: Adding user `weissman' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `weissman' (1001) ...
info: Adding new user `weissman' (1001) with group `weissman (1001)' ...
info: Creating home directory `/home/weissman' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N]
Changing the user information for weissman
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `weissman' to supplemental / extra groups `users' ...
info: Adding user `weissman' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ sudo adduser upper
info: Adding user `upper' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `upper' (1002) ...
info: Adding new user `upper' (1002) with group `upper (1002)' ...
info: Creating home directory `/home/upper' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for upper
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `upper' to supplemental / extra groups `users' ...
info: Adding user `upper' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ sudo adduser lower
info: Adding user `lower' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lower' (1003) ...
info: Adding new user `lower' (1003) with group `lower (1003)' ...
info: Creating home directory `/home/lower' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lower
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `lower' to supplemental / extra groups `users' ...
info: Adding user `lower' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ sudo adduser mixed
info: Adding user `mixed' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `mixed' (1004) ...
info: Adding new user `mixed' (1004) with group `mixed (1004)' ...
info: Creating home directory `/home/mixed' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:

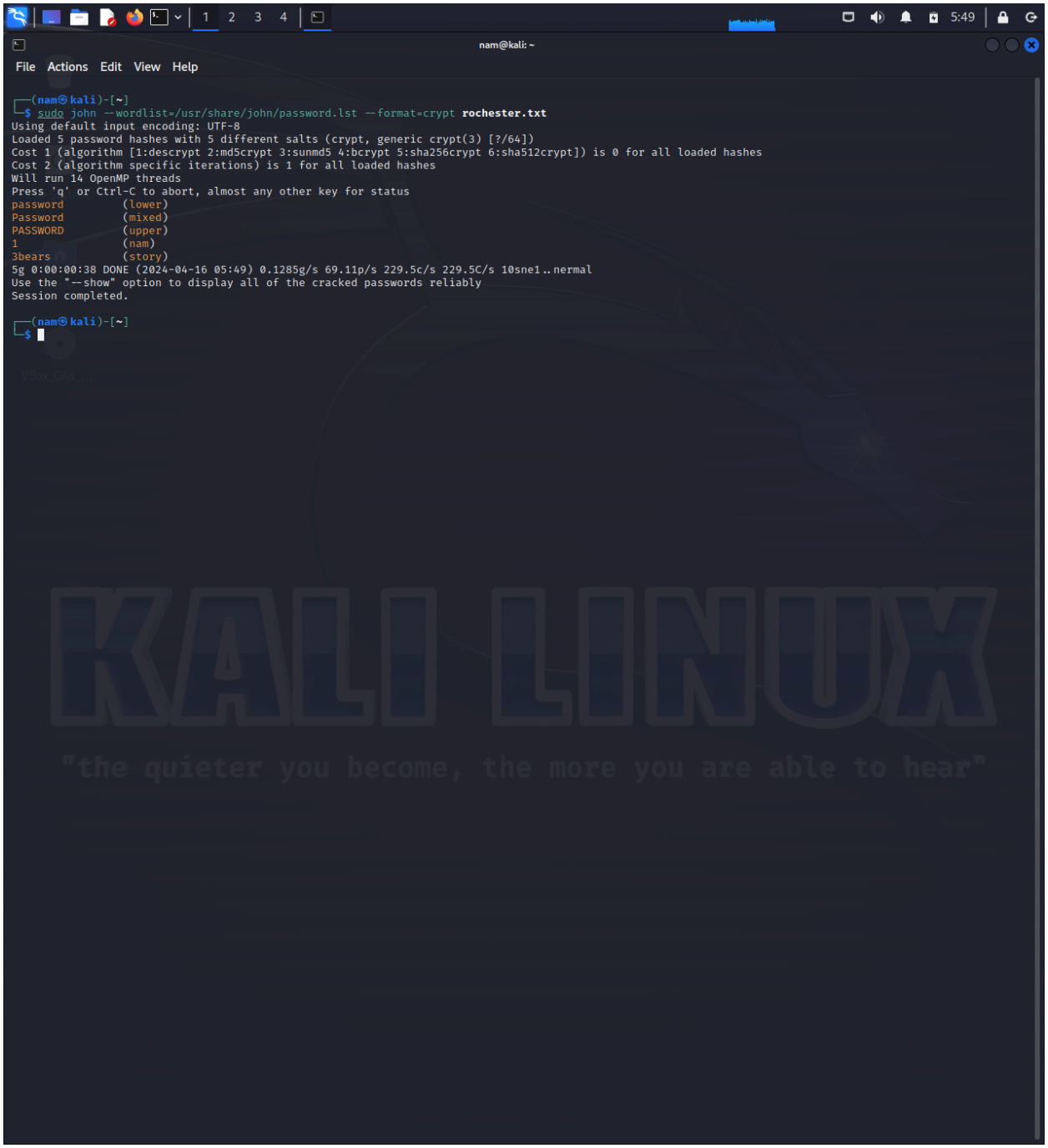

1 2 3 4
5:37
nam@kali: ~
File Actions Edit View Help
Retype new password:
passwd: password updated successfully
Changing the user information for upper
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `upper' to supplemental / extra groups `users' ...
info: Adding user `upper' to group `users' ...
(nam㉿kali)-[~]
$ sudo adduser lower
info: Adding user `lower' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lower' (1003) ...
info: Adding new user `lower' (1003) with group `lower (1003)' ...
info: Creating home directory `/home/lower' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lower
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `lower' to supplemental / extra groups `users' ...
info: Adding user `lower' to group `users' ...
(nam㉿kali)-[~]
$ sudo adduser mixed
info: Adding user `mixed' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `mixed' (1004) ...
info: Adding new user `mixed' (1004) with group `mixed (1004)' ...
info: Creating home directory `/home/mixed' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mixed
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `mixed' to supplemental / extra groups `users' ...
info: Adding user `mixed' to group `users' ...
(nam㉿kali)-[~]
$ sudo adduser story
info: Adding user `story' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `story' (1005) ...
info: Adding new user `story' (1005) with group `story (1005)' ...
info: Creating home directory `/home/story' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for story
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `story' to supplemental / extra groups `users' ...
info: Adding user `story' to group `users' ...
(nam㉿kali)-[~]
$

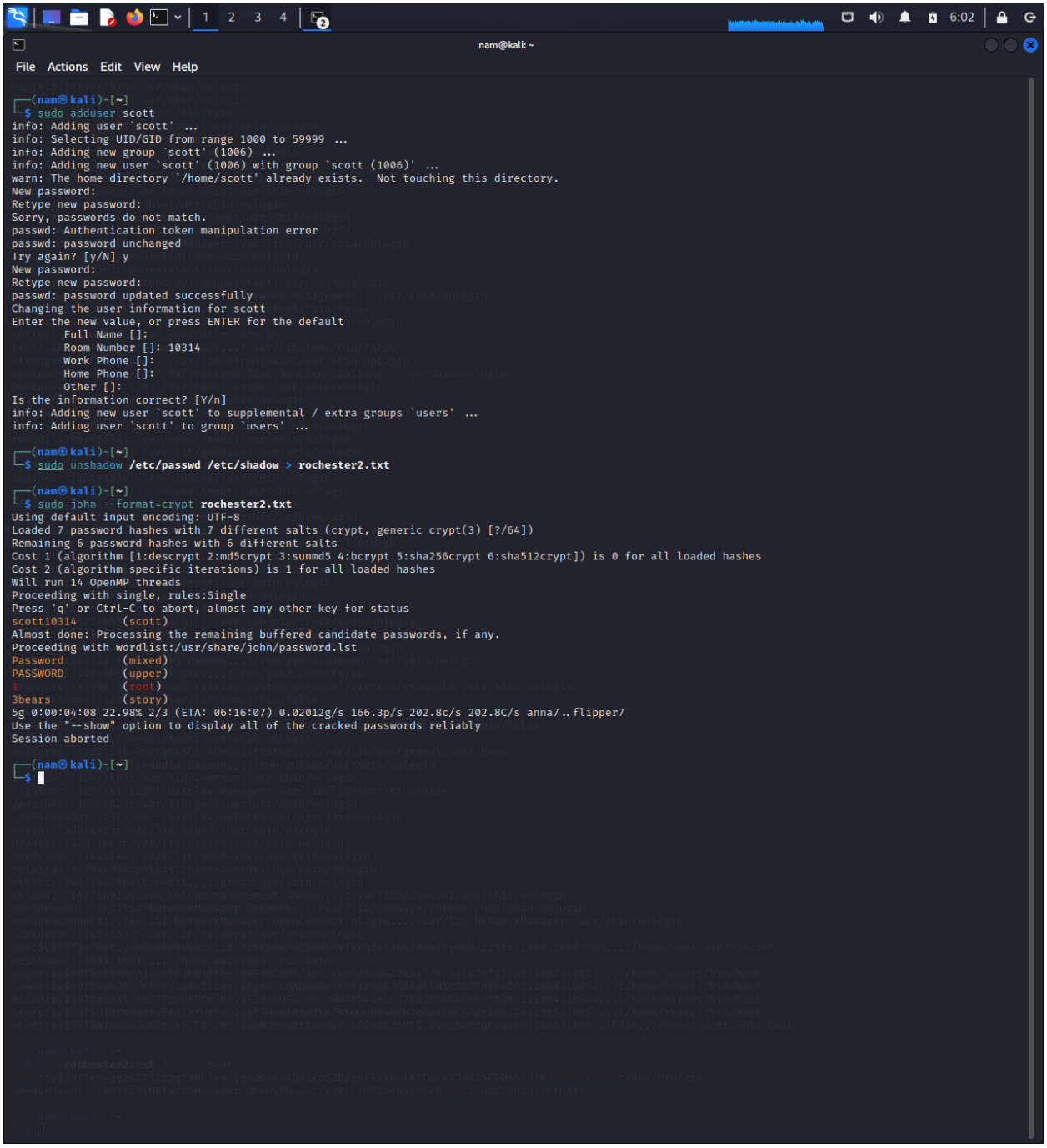

1 2 3 4
5:37
nam@kali: ~
File Actions Edit View Help
info: Adding user `story' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false
_sentrypeer:x:101:108::/var/lib/sentrypeer:/usr/sbin/nologin
cntlm:x:102:65534::/var/run/cntlm:/bin/sh
tss:x:103:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:104:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
Debian-exim:x:105:110::/var/spool/exim4:/usr/sbin/nologin
uuidd:x:106:111::/run/uuidd:/usr/sbin/nologin
debian-tor:x:107:112::/var/lib/tor:/bin/false
redsocks:x:108:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:109:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:110:115::/var/lib/gophish:/usr/sbin/nologin
freerad:x:111:116::/etc/freeradius:/usr/sbin/nologin
iodine:x:112:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:113:117::/nonexistent:/usr/sbin/nologin
clamav:x:114:118::/var/lib/clamav:/bin/false
miredo:x:115:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:116:121::/var/lib/redis:/usr/sbin/nologin
arpwatch:x:117:123:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
usbmux:x:118:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:119:124::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:x:120:126::/nonexistent:/usr/sbin/nologin
sshd:x:121:65534::/run/sshd:/usr/sbin/nologin
_rpc:x:122:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:123:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:124:65534::/var/lib/nfs:/usr/sbin/nologin
freerad-wpe:x:125:130::/etc/freeradius-wpe:/usr/sbin/nologin
avahi:x:126:132:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
gpsd:x:127:20:GPSD system user,,,:/run/gpsd:/bin/false
stunnel4:x:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:128:133::/var/lib/snmp:/bin/false
_gvm:x:129:134::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:130:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:x:131:135::/nonexistent:/usr/sbin/nologin
postgres:x:132:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:x:133:138:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
inetsim:x:134:140::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:135:141:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:x:136:142::/var/lib/geoclue:/usr/sbin/nologin
_defectdojo:x:137:143::/var/log/defectdojo:/usr/sbin/nologin
saned:x:138:145::/var/lib/saned:/usr/sbin/nologin
dradis:x:139:146::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:140:147::/var/lib/beef-xss:/usr/sbin/nologin
polkitd:x:994:994:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:141:148:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:142:149:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:143:150:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:144:151:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
_caldera:x:145:153::/var/lib/caldera:/usr/sbin/nologin
nam:x:1000:1000:nam,,,:/home/nam:/usr/bin/zsh
weissman:x:1001:1001:,,,:/home/weissman:/bin/bash
upper:x:1002:1002:,,,:/home/upper:/bin/bash
lower:x:1003:1003:,,,:/home/lower:/bin/bash
mixed:x:1004:1004:,,,:/home/mixed:/bin/bash
story:x:1005:1005:,,,:/home/story:/bin/bash
┌──(nam㉿kali)-[~]
└─$

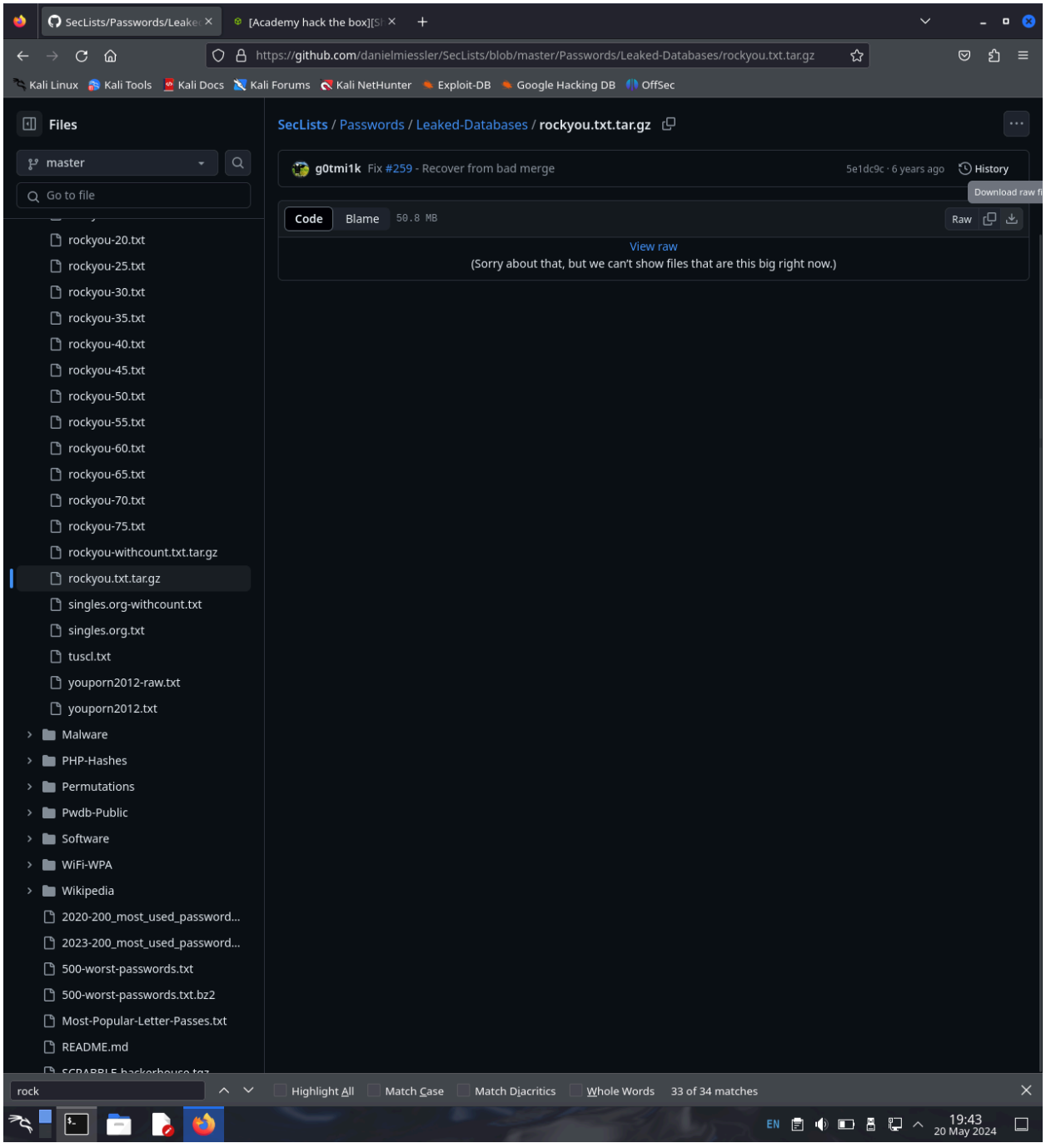

1 2 3 4
5:37
nam@kali: ~
File Actions Edit View Help
story:x:1005:1005:,,,:/home/story:/bin/bash
(nam㉿kali)-[~]
$ sudo cat /etc/shadow
root:!:19816:0:99999:7:::
daemon:*:19816:0:99999:7:::
bin:*:19816:0:99999:7:::
sys:*:19816:0:99999:7:::
sync:*:19816:0:99999:7:::
games:*:19816:0:99999:7:::
man:*:19816:0:99999:7:::
lp:*:19816:0:99999:7:::
mail:*:19816:0:99999:7:::
news:*:19816:0:99999:7:::
uucp:*:19816:0:99999:7:::
proxy:*:19816:0:99999:7:::
www-data:*:19816:0:99999:7:::
backup:*:19816:0:99999:7:::
list:*:19816:0:99999:7:::
irc:*:19816:0:99999:7:::
_apt:*:19816:0:99999:7:::
nobody:*:19816:0:99999:7:::
systemd-network:!*:19816::::::
mysql:!:19816::::::
_sentrypeer:!:19816::::::
cntlm:!:19816::::::
tss:!:19816::::::
strongswan:!:19816::::::
systemd-timesync:!*:19816::::::
Debian-exim:!:19816::::::
uuidd:!:19816::::::
debian-tor:!:19816::::::
redsocks:!:19816::::::
rwhod:!:19816::::::
_gophish:!:19816::::::
freerad:!:19816::::::
iodine:!:19816::::::
messagebus:!:19816::::::
clamav:!:19816::::::
miredo:!:19816::::::
redis:!:19816::::::
arpwatch:!:19816::::::
usbmux:!:19816::::::
mosquitto:!:19816::::::
tcpdump:!:19816::::::
sshd:!:19816::::::
_rpc:!:19816::::::
dnsmasq:!:19816::::::
statd:!:19816::::::
freerad-wpe:!:19816::::::
avahi:!:19816::::::
gpsd:!:19816::::::
stunnel4:!*:19816::::::
Debian-snmp:!:19816::::::
_gvm:!:19816::::::
speech-dispatcher:!:19816::::::
sslh:!:19816::::::
postgres:!:19816::::::
pulse:!:19816::::::
inetsim:!:19816::::::
lightdm:!:19816::::::
geoclue:!:19816::::::
_defectdojo:!:19816::::::
saned:!:19816::::::
dradis:!:19816::::::
beef-xss:!:19816::::::
polkitd:!*:19816::::::
rtkit:!:19816::::::
colord:!:19816::::::
nm-openvpn:!:19816::::::
nm-openconnect:!:19816::::::
_caldera:!:19816::::::
nam:yj9T$gCNiceYNwtaT46cyHt5FZ0$wXQKQacCe//hT1tBqOiAZyi/spr8ydKYzyMOpNnLfi7:19816:0:99999:7:::
weissman:!:19829:0:99999:7:::
upper:yj9T$pFVFmcpj3ph55JbWjBfhF/$9F3GCnM1/3p1/Ipp5aSkqGZzi5ij7k.3gly2GTg7jq6:19829:0:99999:7:::
lower:yj9T$syOJhx/mfhK/1pRnZ1L0r.$Dg8R.L0WNWWBa/Xmfir5qE/Q2cg6lH1CZDJTHfB4ZO7:19829:0:99999:7:::
mixed:yj9T$p9axl/KesTP2vVRPSm/NR.$FIdnbQF./Sm/rMWAY54cmlrJ7LWJBbkNwEVk/Y5qto1:19829:0:99999:7:::
story:yj9T$N19KW9ydzyEtRiaYUtfaO1$gt7QcKKM5ddkeFAtQOUDzwDKH2oGpA1eCG2gt2Rp.ZA:19829:0:99999:7:::
(nam㉿kali)-[~]
$

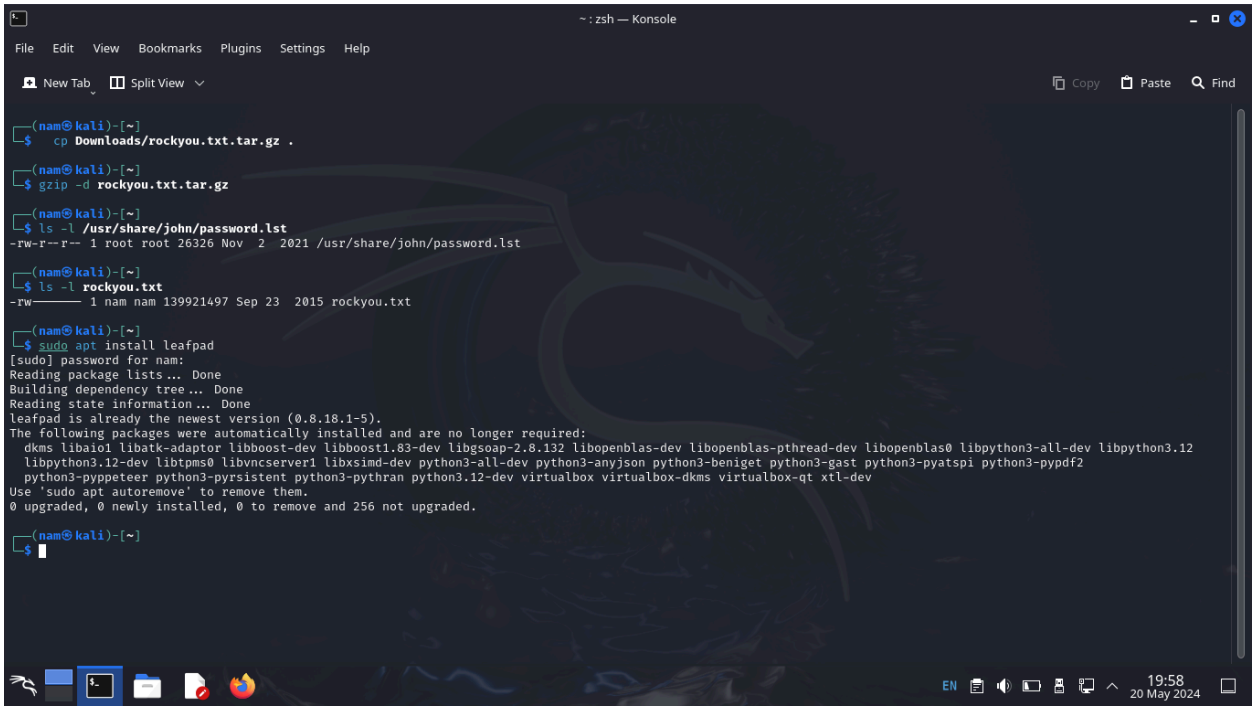

1 2 3 4
5:38
nam@kali: ~
File Actions Edit View Help
UNSHADOW(8) System Manager's Manual UNSHADOW(8)
NAME
unshadow - combines passwd and shadow files
SYNOPSIS
unshadow password-file shadow-file
DESCRIPTION
This manual page documents briefly the unshadow command, which is part of the john package. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. john, better known as John the Ripper, is a tool to find weak passwords of users in a server.
The unshadow tool combines the passwd and shadow files so John can use them. You might need this since if you only used your shadow file, the GECOS information wouldn't be used by the "single crack" mode, and also you wouldn't be able to use the '-shells' option. On a normal system you'll need to run unshadow as root to be able to read the shadow file.
SEE ALSO
john(8), mailer(8), unafs(8), unique(8).
The programs are documented fully by John's documentation, which should be available in /usr/share/doc/john or other location, depending on your system.
AUTHOR
This manual page was written by Jordi Mallach <jordi@debian.org>, for the Debian GNU/Linux system (but may be used by others).
John the Ripper and mailer were written by Solar Designer <solar@openwall.com>. The complete list of contributors can be found in the CREDITS file in the documentation directory.
john June 03, 2004 UNSHADOW(8)
Manual page unshadow(8) line 1/29 (END) (press h for help or q to quit)
KALI LINUX
"the quieter you become, the more you are able to hear"

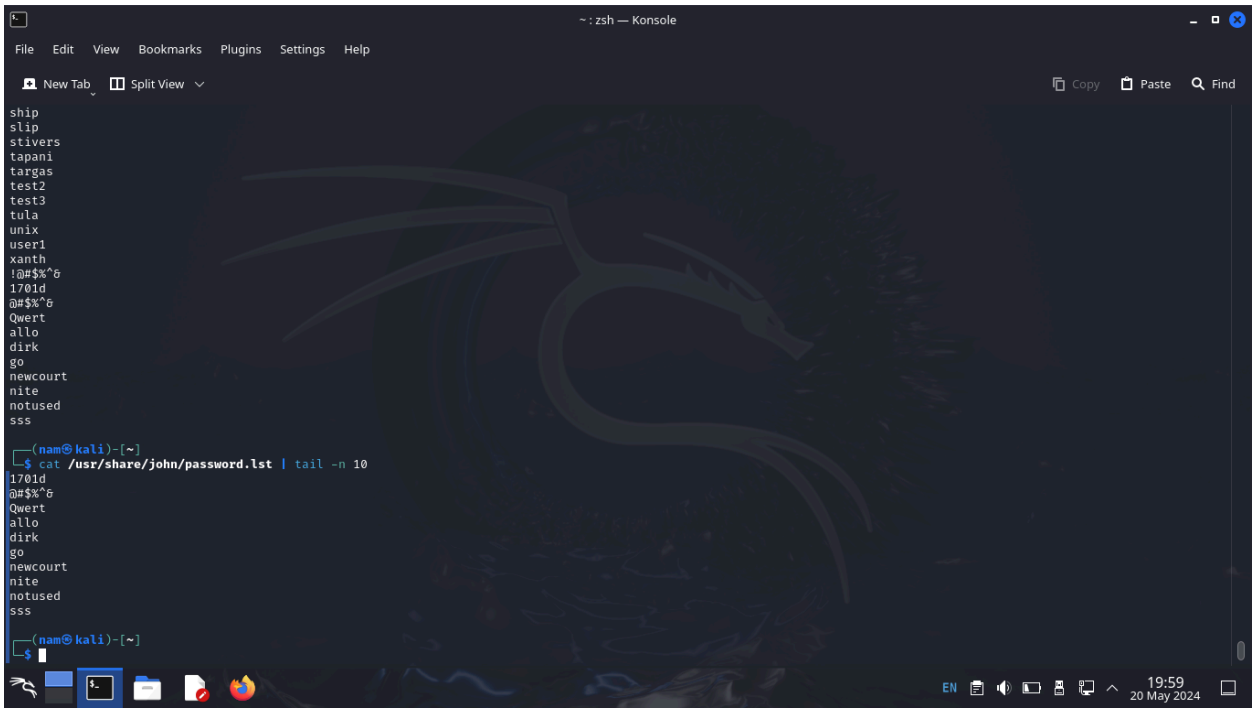

1 2 3 4
5:39
nam@kali: ~
File Actions Edit View Help
└─$ sudo unshadow /etc/passwd /etc/shadow >rochester.txt
┌──(nam㉿kali)-[~]
└─$ cat rochester.txt
root:!:0:0:root:/root:/usr/bin/zsh
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:*:42:65534::/nonexistent:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:!*:998:998:systemd Network Management:/:/usr/sbin/nologin
mysql:!:100:107:MySQL Server,,,:/nonexistent:/bin/false
_sentrypeer:!:101:108::/var/lib/sentrypeer:/usr/sbin/nologin
cntlm:!:102:65534::/var/run/cntlm:/bin/sh
tss:!:103:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:!:104:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:!*:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
Debian-exim:!:105:110::/var/spool/exim4:/usr/sbin/nologin
uuidd:!:106:111::/run/uuidd:/usr/sbin/nologin
debian-tor:!:107:112::/var/lib/tor:/bin/false
redsocks:!:108:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:!:109:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:!:110:115::/var/lib/gophish:/usr/sbin/nologin
freerad:!:111:116::/etc/freeradius:/usr/sbin/nologin
iodine:!:112:65534::/run/iodine:/usr/sbin/nologin
messagebus:!:113:117::/nonexistent:/usr/sbin/nologin
clamav:!:114:118::/var/lib/clamav:/bin/false
miredo:!:115:65534::/var/run/miredo:/usr/sbin/nologin
redis:!:116:121::/var/lib/redis:/usr/sbin/nologin
arpwatch:!:117:123:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
usbmux:!:118:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:!:119:124::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:!:120:126::/nonexistent:/usr/sbin/nologin
sshd:!:121:65534::/run/sshd:/usr/sbin/nologin
_rpc:!:122:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:!:123:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:!:124:65534::/var/lib/nfs:/usr/sbin/nologin
freerad-wpe:!:125:130::/etc/freeradius-wpe:/usr/sbin/nologin
avahi:!:126:132:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
gpsd:!:127:20:GPSD system user,,,:/run/gpsd:/bin/false
stunnel4:!*:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:!:128:133::/var/lib/snmp:/bin/false
_gvm:!:129:134::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:!:130:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:!:131:135::/nonexistent:/usr/sbin/nologin
postgres:!:132:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:!:133:138:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
inetsim:!:134:140::/var/lib/inetsim:/usr/sbin/nologin
lightdm:!:135:141:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:!:136:142::/var/lib/geoclue:/usr/sbin/nologin
_defectdojo:!:137:143::/var/log/defectdojo:/usr/sbin/nologin
saned:!:138:145::/var/lib/saned:/usr/sbin/nologin
dradis:!:139:146::/var/lib/dradis:/usr/sbin/nologin
beef-xss:!:140:147::/var/lib/beef-xss:/usr/sbin/nologin
polkitd:!*:994:994:polkit:/nonexistent:/usr/sbin/nologin
rtkit:!:141:148:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:!:142:149:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:!:143:150:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:!:144:151:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
_caldera:!:145:153::/var/lib/caldera:/usr/sbin/nologin
nam:yj9T$gCNiceYNwtaT46cyHt5FZ0$wXQKQacCe//hT1tBqOiAZyi/spr8ydKYzyMOpNnLfi7:1000:1000:nam,,,:/home/nam:/usr/bin/zsh
weissman:!:1001:1001:,,,:/home/weissman:/bin/bash
upper:yj9T$pFVFmcpj3ph55JbWjBfhF/$9F3GCnM1/3p1/Ipp5aSkqGZzi5ij7k.3gly2GTg7jq6:1002:1002:,,,:/home/upper:/bin/bash
lower:yj9T$syOJhx/mfhK/1pRnZ1L0r.$Dg8R.L0WNWWBa/Xmfir5qE/Q2cg6lH1CZDJTHfB4ZO7:1003:1003:,,,:/home/lower:/bin/bash
mixed:yj9T$p9axl/KesTP2vVRPSm/NR.$FIdnbQF./Sm/rMWAY54cmlrJ7LWJBbkNwEVk/Y5qto1:1004:1004:,,,:/home/mixed:/bin/bash
story:yj9T$N19KW9ydzyEtRiaYUtfaO1$gt7QcKKM5ddkeFAtQOUDzwDKH2oGpA1eCG2gt2Rp.ZA:1005:1005:,,,:/home/story:/bin/bash
┌──(nam㉿kali)-[~]
└─$

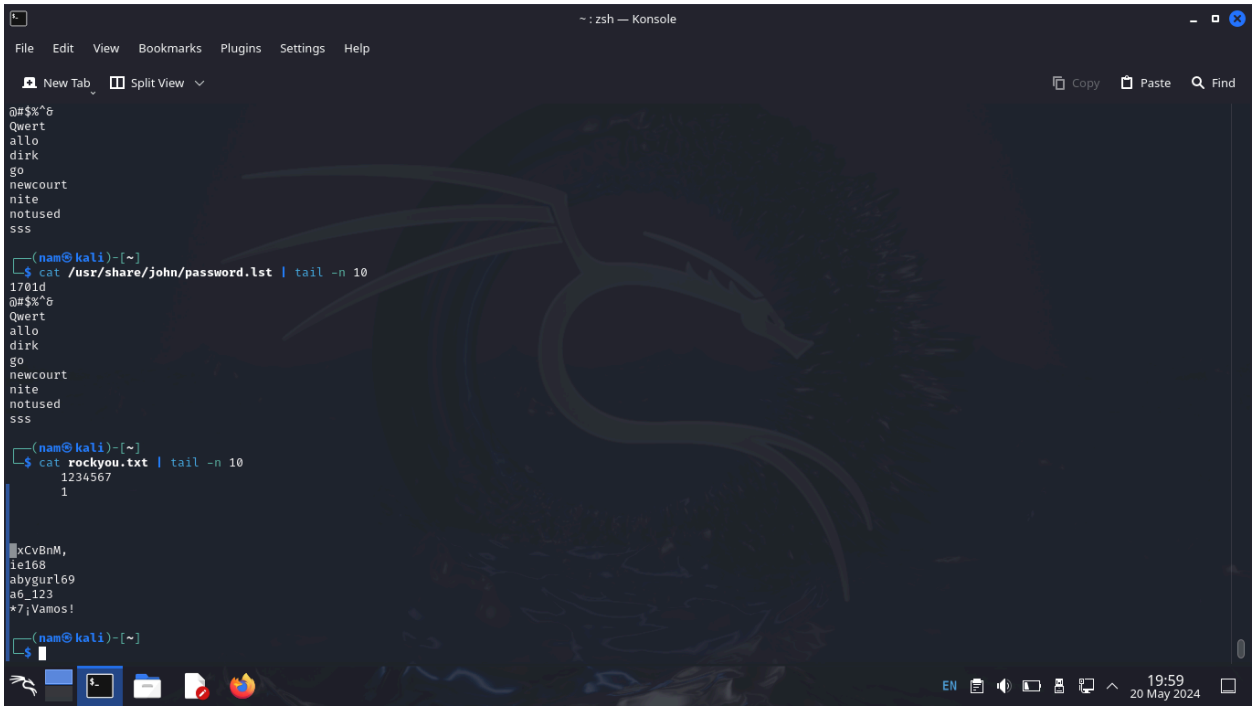

1 2 3 4
5:49
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo john --wordlist=/usr/share/john/password.lst --format=crypt rochester.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 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 14 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (lower)
Password (mixed)
PASSWORD (upper)
1 (nam)
3bears (story)
5g 0:00:00:38 DONE (2024-04-16 05:49) 0.1285g/s 69.11p/s 229.5c/s 229.5C/s 10sne1..nermal
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(nam㉿kali)-[~]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"

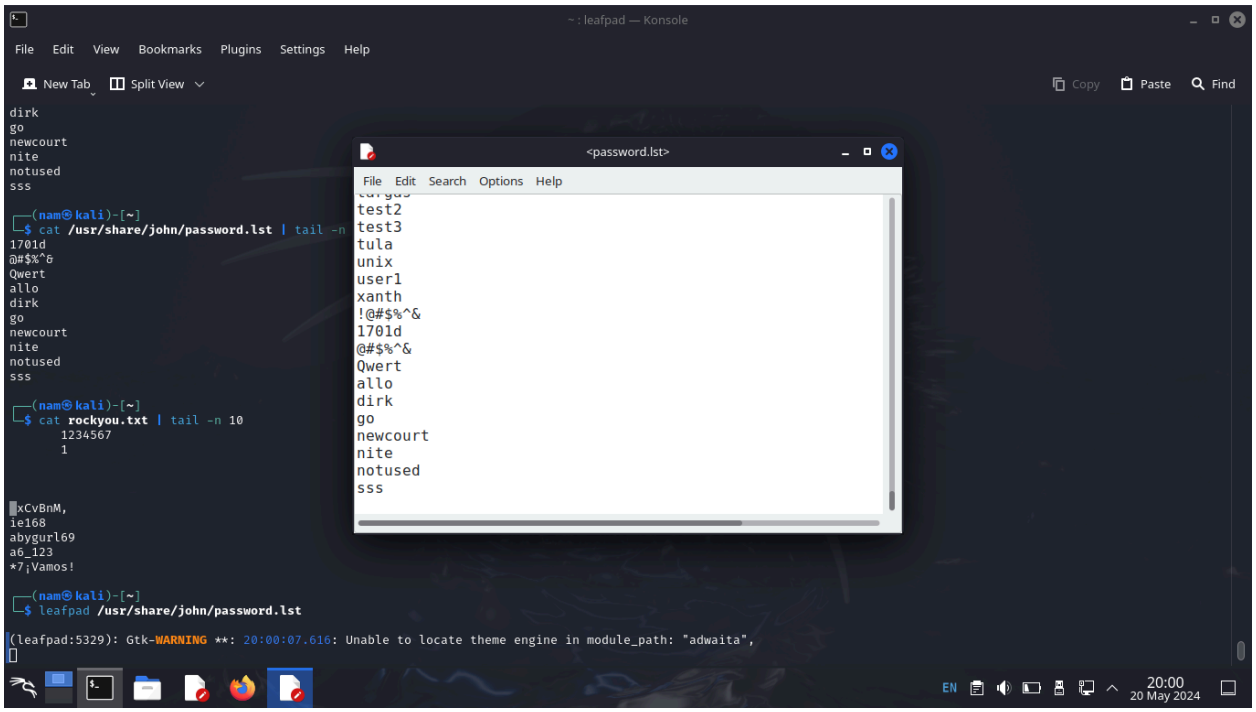

1 2 3 4
6:02
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo adduser scott
info: Adding user `scott' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `scott' (1006) ...
info: Adding new user `scott' (1006) with group `scott (1006)' ...
warn: The home directory `/home/scott' already exists. Not touching this directory.
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for scott
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []: 10314
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `scott' to supplemental / extra groups `users' ...
info: Adding user `scott' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > rochester2.txt
┌──(nam㉿kali)-[~]
└─$ sudo john --format=crypt rochester2.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Remaining 6 password hashes with 6 different salts
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 14 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
scott10314 (scott)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Password (mixed)
PASSWORD (upper)
1 (root)
3bears (story)
5g 0:00:04:08 22.98% 2/3 (ETA: 06:16:07) 0.02012g/s 166.3p/s 202.8c/s 202.8C/s anna7..flipper7
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
┌──(nam㉿kali)-[~]
└─$

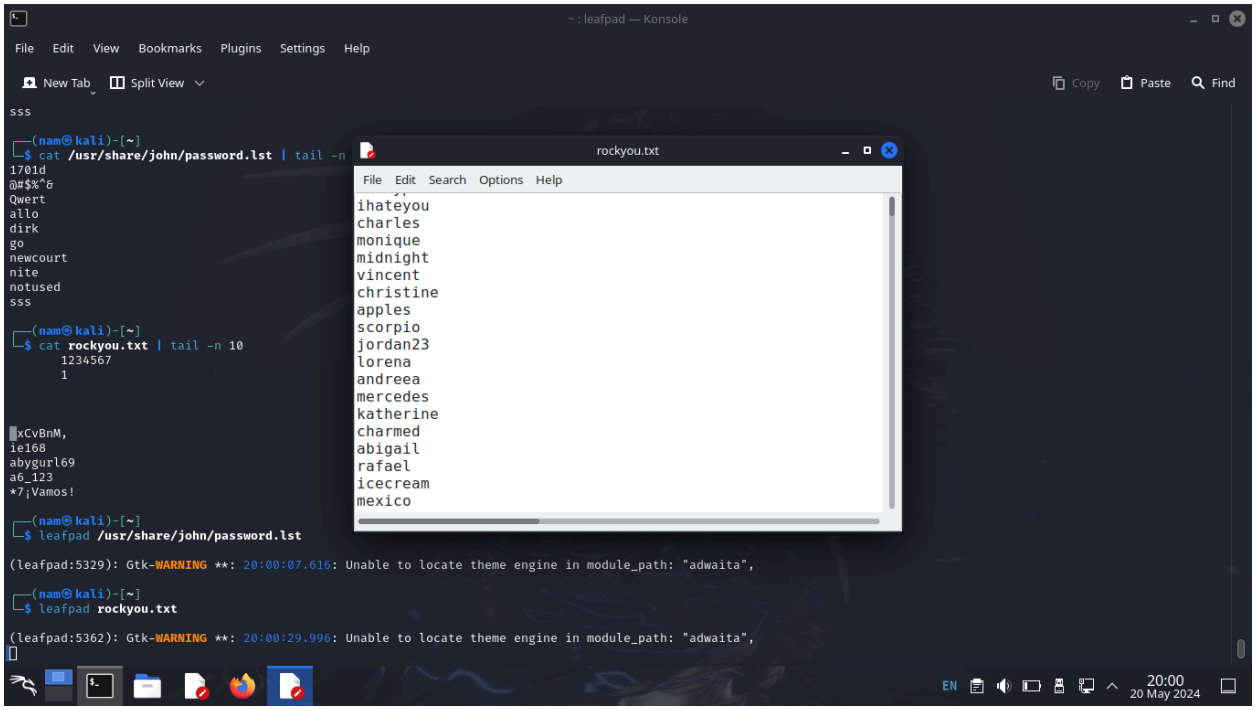

SecLists/Passwords/Leake
[Academy hack the box][Sl
https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Files
master
Go to file
rockyou-20.txt
rockyou-25.txt
rockyou-30.txt
rockyou-35.txt
rockyou-40.txt
rockyou-45.txt
rockyou-50.txt
rockyou-55.txt
rockyou-60.txt
rockyou-65.txt
rockyou-70.txt
rockyou-75.txt
rockyou-withcount.txt.tar.gz
rockyou.txt.tar.gz
singles.org-withcount.txt
singles.org.txt
tuscl.txt
youporn2012-raw.txt
youporn2012.txt
Malware
PHP-Hashes
Permutations
Pwdb-Public
Software
WiFi-WPA
Wikipedia
2020-200_most_used_password...
2023-200_most_used_password...
500-worst-passwords.txt
500-worst-passwords.txt.bz2
Most-Popular-Letter-Passes.txt
README.md
SecLists / Passwords / Leaked-Databases / rockyou.txt.tar.gz
g0tmi1k Fix #259 - Recover from bad merge
5e1dc9c · 6 years ago
History
Download raw fi
Code
Blame
50.8 MB
Raw
View raw
(Sorry about that, but we can't show files that are this big right now.)
rock
Highlight All
Match Case
Match Diacritics
Whole Words
33 of 34 matches
EN
19:43
20 May 2024

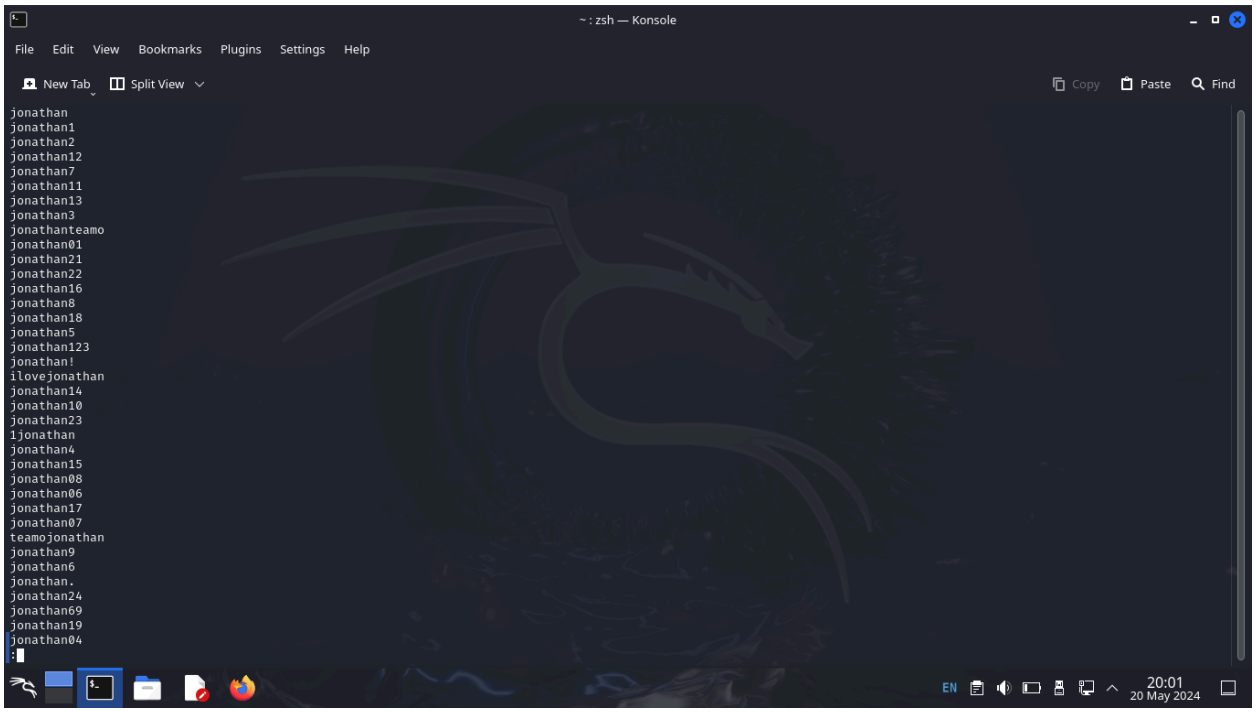

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ cp Downloads/rockyou.txt.tar.gz .
┌──(nam㉿kali)-[~]
└─$ gzip -d rockyou.txt.tar.gz
┌──(nam㉿kali)-[~]
└─$ ls -l /usr/share/john/password.lst
-rw-r--r-- 1 root root 26326 Nov 2 2021 /usr/share/john/password.lst
┌──(nam㉿kali)-[~]
└─$ ls -l rockyou.txt
-rw------- 1 nam nam 139921497 Sep 23 2015 rockyou.txt
┌──(nam㉿kali)-[~]
└─$ sudo apt install leafpad
[sudo] password for nam:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
leafpad is already the newest version (0.8.18.1-5).
The following packages were automatically installed and are no longer required:
dkms libaio1 libatk-adaptor libboost-dev libboost1.83-dev libgsoap-2.8.132 libopenblas-dev libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12
libpython3.12-dev libtpms0 libvncserver1 libxsimd-dev python3-all-dev python3-anyjson python3-beniget python3-gast python3-pyatspi python3-pypdf2
python3-pyppeteer python3-pyrsistent python3-pythran python3.12-dev virtualbox virtualbox-dkms virtualbox-qt xtl-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 256 not upgraded.
┌──(nam㉿kali)-[~]
└─$
EN 19:58 20 May 2024

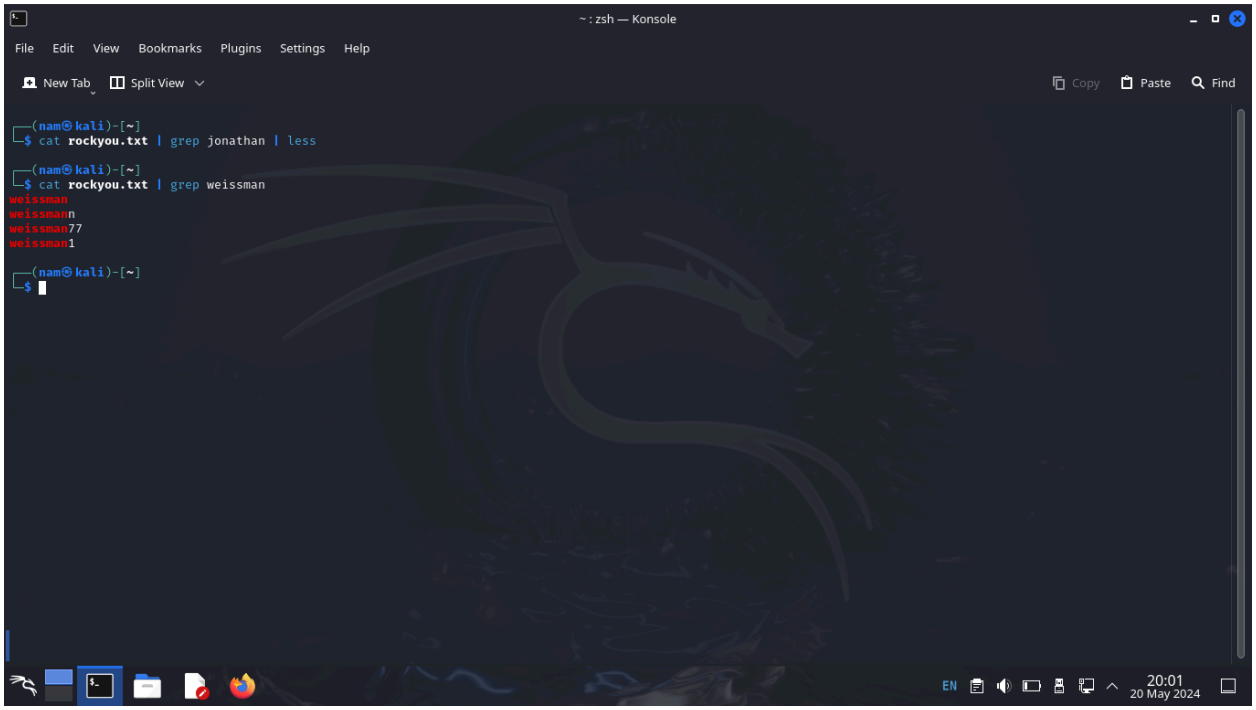

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
ship
slip
stivers
tapani
targas
test2
test3
tula
unix
user1
xanth
!@#$%^&
1701d
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$ cat /usr/share/john/password.lst | tail -n 10
1701d
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$
EN 19:59 20 May 2024

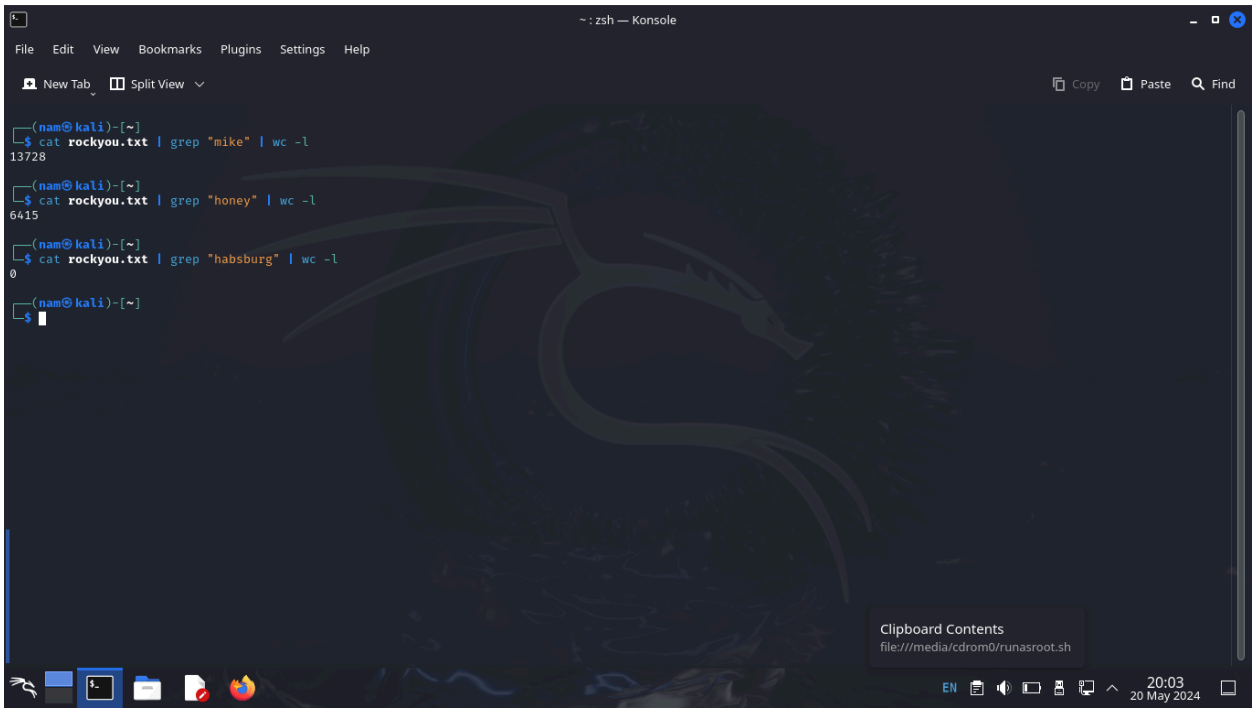

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$ cat /usr/share/john/password.lst | tail -n 10
1701d
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | tail -n 10
1234567
1
xCvBnM,
1e168
abygurl69
a6_123
*7¡Vamos!
┌──(nam㉿kali)-[~]
└─$
EN
19:59
20 May 2024

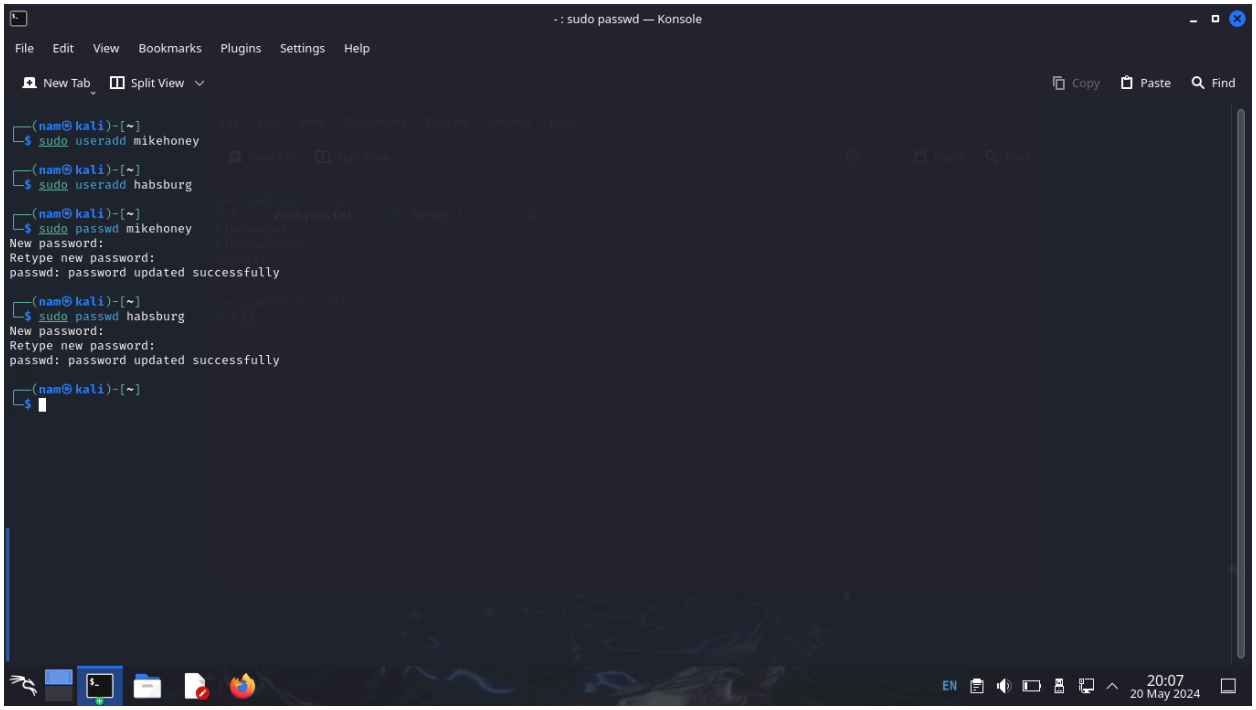

~ : leafpad — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$ cat /usr/share/john/password.lst | tail -n
1701d
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | tail -n 10
1234567
1
xCvBnM,
1e168
abygurl69
a6_123
*7¡Vamos!
┌──(nam㉿kali)-[~]
└─$ leafpad /usr/share/john/password.lst
(leafpad:5329): Gtk-WARNING **: 20:00:07.616: Unable to locate theme engine in module_path: "adwaita",
<password.lst>
File Edit Search Options Help
test2
test3
tula
unix
user1
xanth
!@#$%^&
1701d
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
EN
20:00
20 May 2024

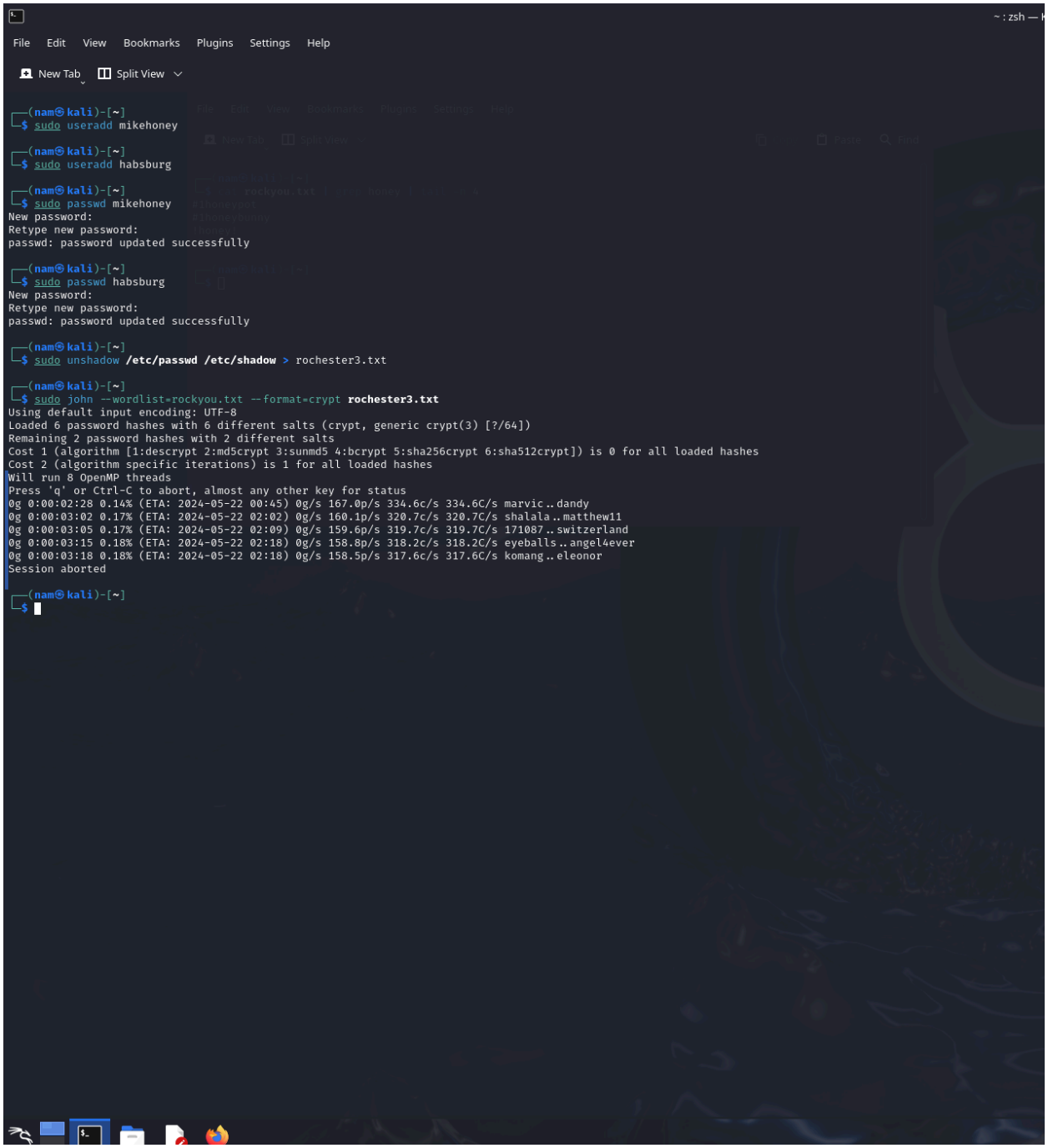

~ : leafpad — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
sss
┌──(nam㉿kali)-[~]
└─$ cat /usr/share/john/password.lst | tail -n
1701d
@#$%^&
Qwert
allo
dirk
go
newcourt
nite
notused
sss
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | tail -n 10
1234567
1
xCvBnM,
ie168
abygurl69
a6_123
*7¡Vamos!
┌──(nam㉿kali)-[~]
└─$ leafpad /usr/share/john/password.lst
(leafpad:5329): Gtk-WARNING **: 20:00:07.616: Unable to locate theme engine in module_path: "adwaita",
┌──(nam㉿kali)-[~]
└─$ leafpad rockyou.txt
(leafpad:5362): Gtk-WARNING **: 20:00:29.996: Unable to locate theme engine in module_path: "adwaita",
rockyou.txt
File Edit Search Options Help
ihateyou
charles
monique
midnight
vincent
christine
apples
scorpio
jordan23
lorena
andreea
mercedes
katherine
charmed
abigail
rafael
icecream
mexico
EN
20:00
20 May 2024


~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
jonathan
jonathan1
jonathan2
jonathan12
jonathan7
jonathan11
jonathan13
jonathan3
jonathanteamo
jonathan01
jonathan21
jonathan22
jonathan16
jonathan8
jonathan18
jonathan5
jonathan123
jonathan!
ilovejonathan
jonathan14
jonathan10
jonathan23
1jonathan
jonathan4
jonathan15
jonathan08
jonathan06
jonathan17
jonathan07
teamojonathan
jonathan9
jonathan6
jonathan.
jonathan24
jonathan69
jonathan19
jonathan04
EN
20:01
20 May 2024


~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | grep jonathan | less
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | grep weissman
weissman
weissmann
weissman77
weissman1
┌──(nam㉿kali)-[~]
└─$
EN
20:01
20 May 2024

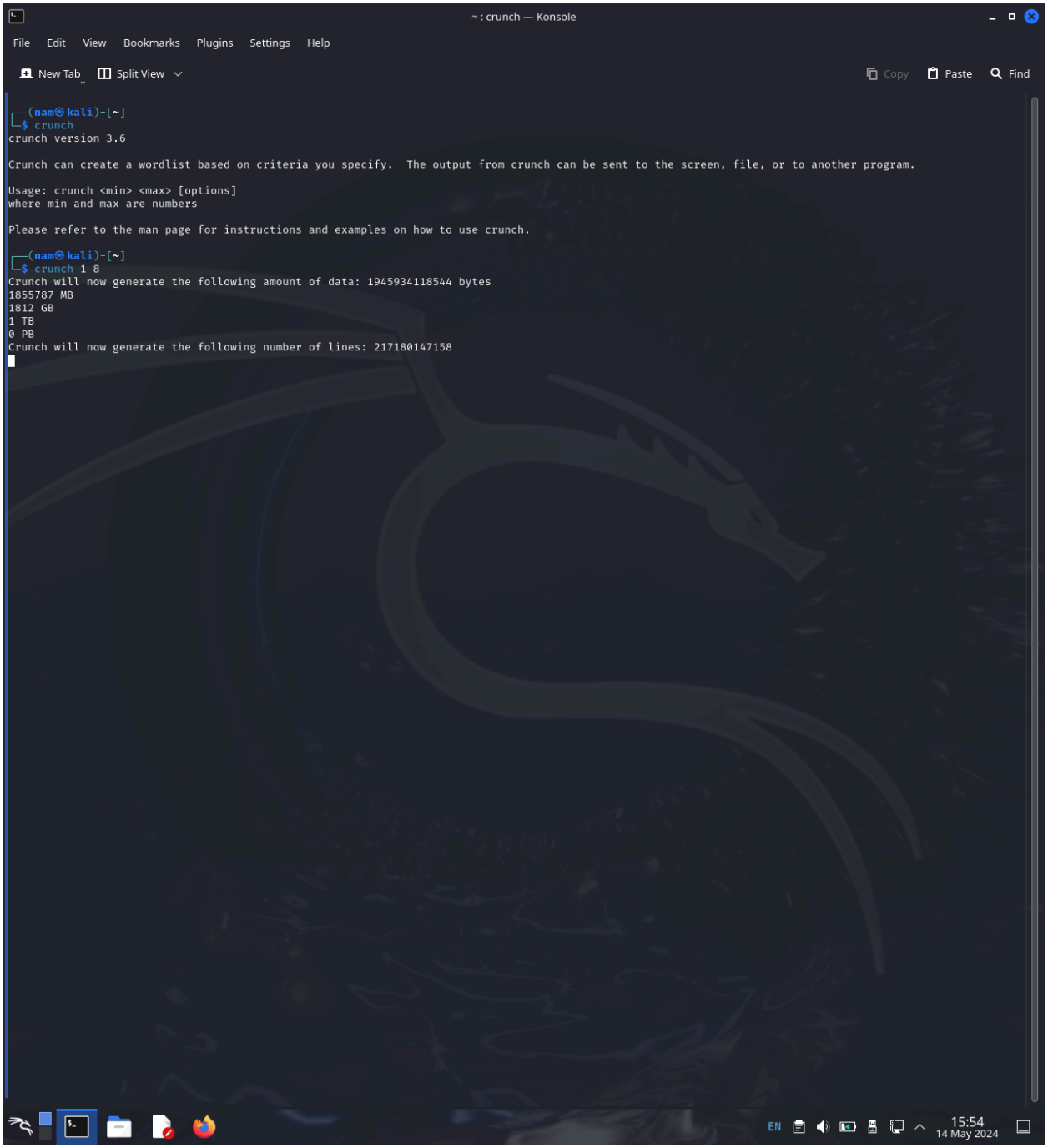

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | grep "mike" | wc -l
13728
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | grep "honey" | wc -l
6415
┌──(nam㉿kali)-[~]
└─$ cat rockyou.txt | grep "habsburg" | wc -l
0
┌──(nam㉿kali)-[~]
└─$
Clipboard Contents
file:///media/cdrom0/runasroot.sh
EN
20:03
20 May 2024

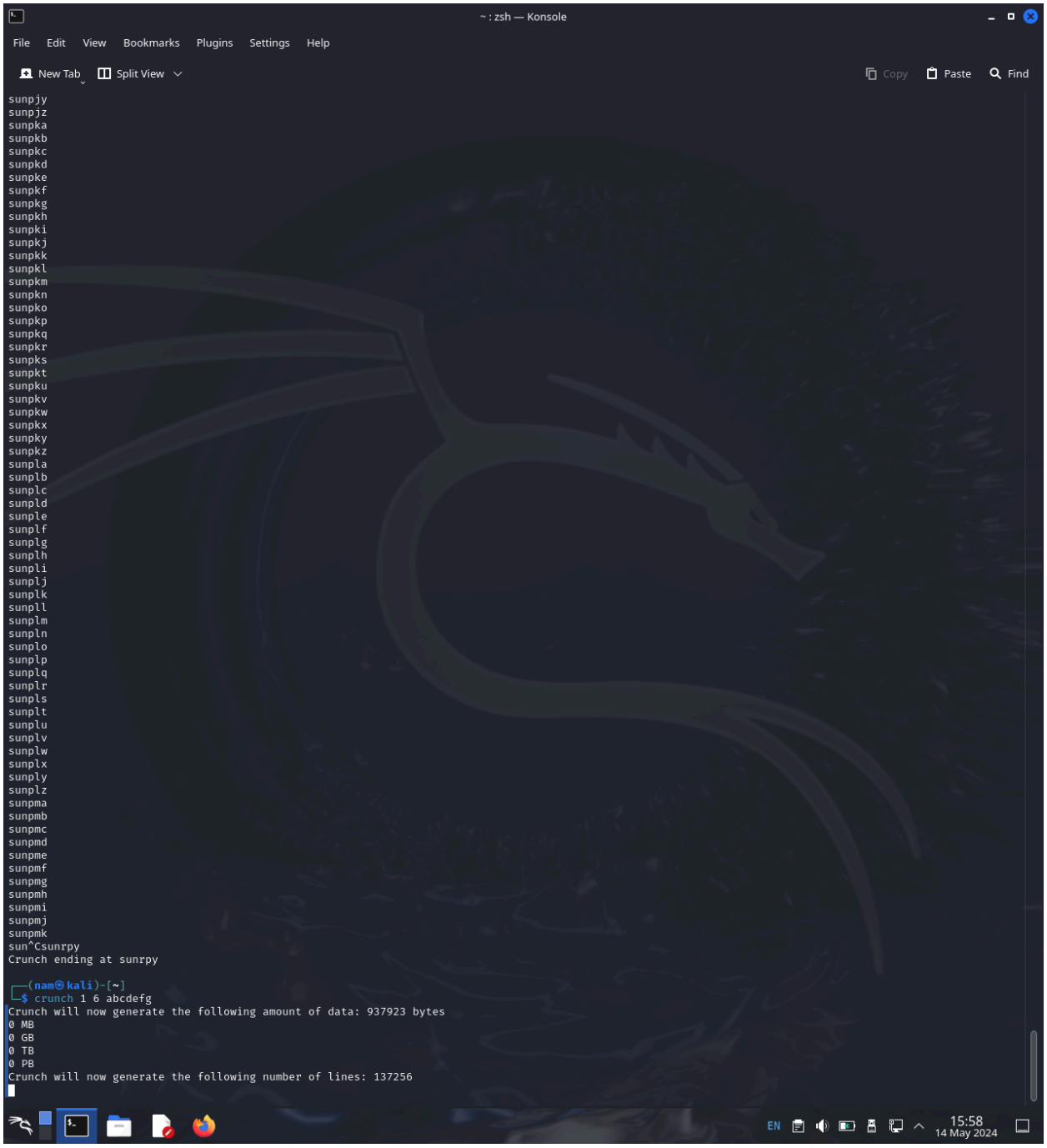

- : sudo passwd — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo useradd mikehoney
┌──(nam㉿kali)-[~]
└─$ sudo useradd habsburg
┌──(nam㉿kali)-[~]
└─$ sudo passwd mikehoney
New password:
Retype new password:
passwd: password updated successfully
┌──(nam㉿kali)-[~]
└─$ sudo passwd habsburg
New password:
Retype new password:
passwd: password updated successfully
┌──(nam㉿kali)-[~]
└─$
EN
20:07
20 May 2024

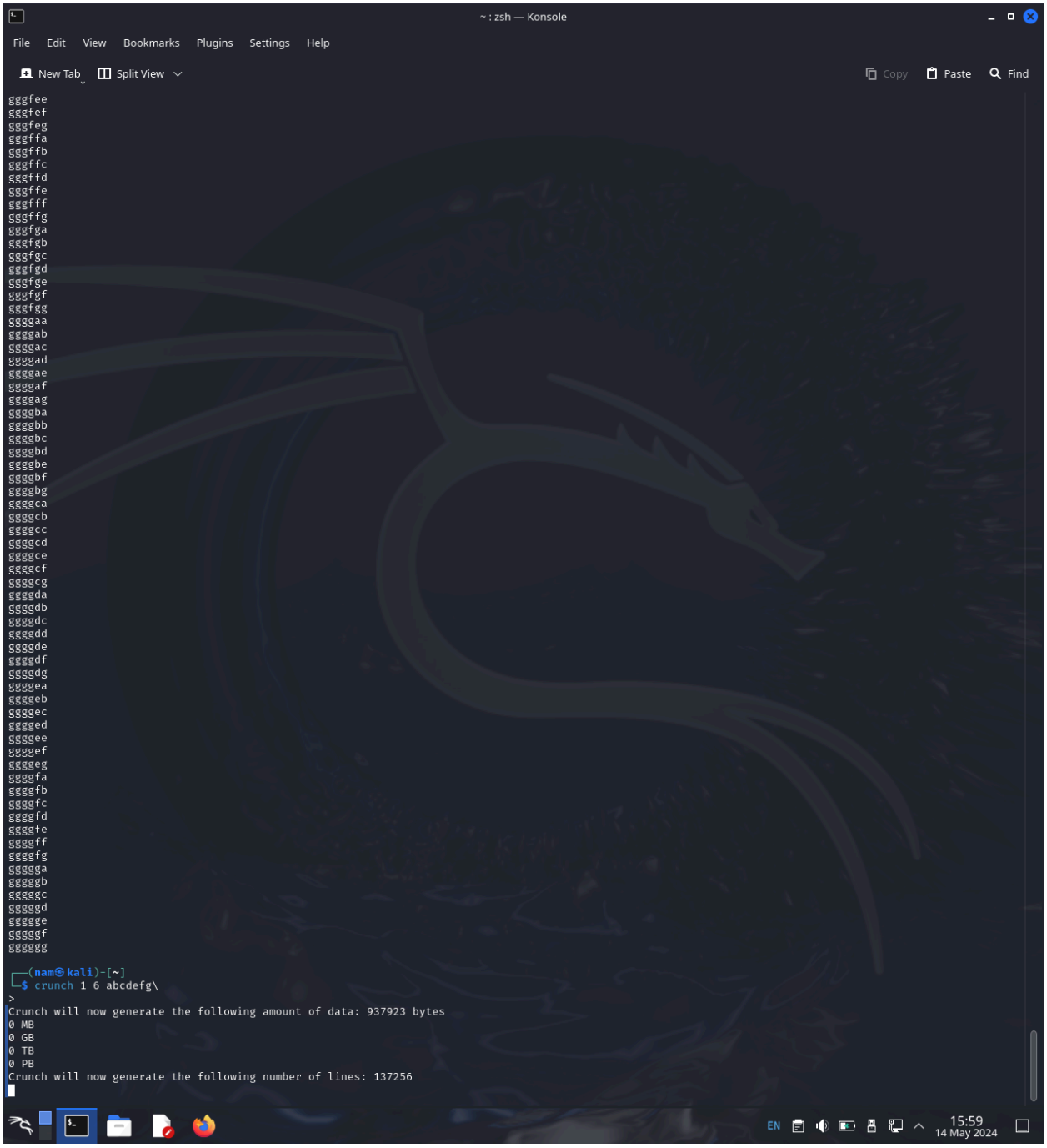

File Edit View Bookmarks Plugins Settings Help
New Tab Split View
(nam㉿kali)-[~]
$ sudo useradd mikehoney
(nam㉿kali)-[~]
$ sudo useradd habsburg
(nam㉿kali)-[~]
$ sudo passwd mikehoney
New password:
Retype new password:
passwd: password updated successfully
(nam㉿kali)-[~]
$ sudo passwd habsburg
New password:
Retype new password:
passwd: password updated successfully
(nam㉿kali)-[~]
$ sudo unshadow /etc/passwd /etc/shadow > rochester3.txt
(nam㉿kali)-[~]
$ sudo john --wordlist=rockyou.txt --format=crypt rochester3.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Remaining 2 password hashes with 2 different salts
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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:28 0.14% (ETA: 2024-05-22 00:45) 0g/s 167.0p/s 334.6c/s 334.6C/s marvic..dandy
0g 0:00:03:02 0.17% (ETA: 2024-05-22 02:02) 0g/s 160.1p/s 320.7c/s 320.7C/s shalala..matthew11
0g 0:00:03:05 0.17% (ETA: 2024-05-22 02:09) 0g/s 159.6p/s 319.7c/s 319.7C/s 171087..switzerland
0g 0:00:03:15 0.18% (ETA: 2024-05-22 02:18) 0g/s 158.8p/s 318.2c/s 318.2C/s eyeballs..angel4ever
0g 0:00:03:18 0.18% (ETA: 2024-05-22 02:18) 0g/s 158.5p/s 317.6c/s 317.6C/s komang..eleonor
Session aborted
(nam㉿kali)-[~]
$

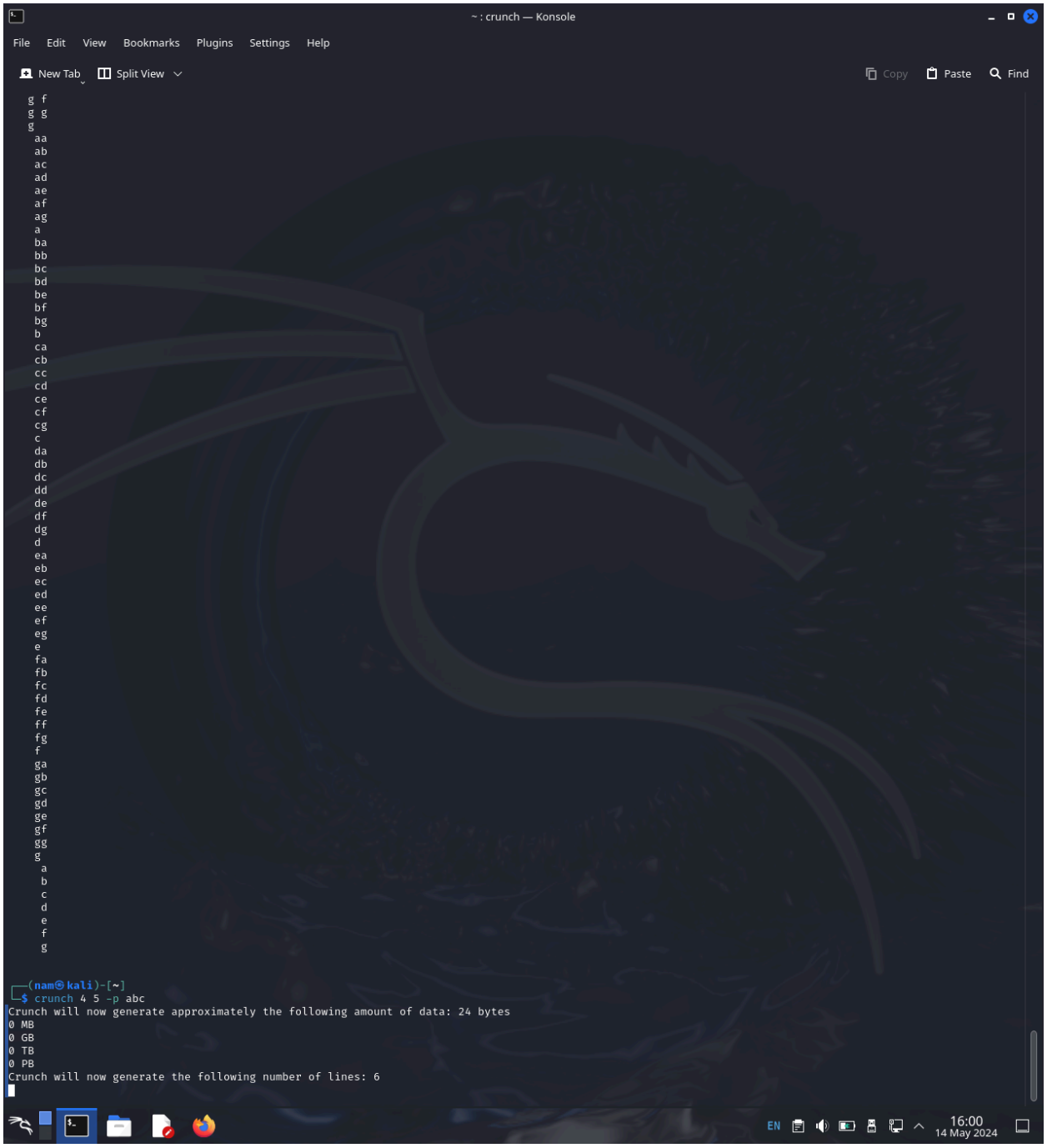
11.02

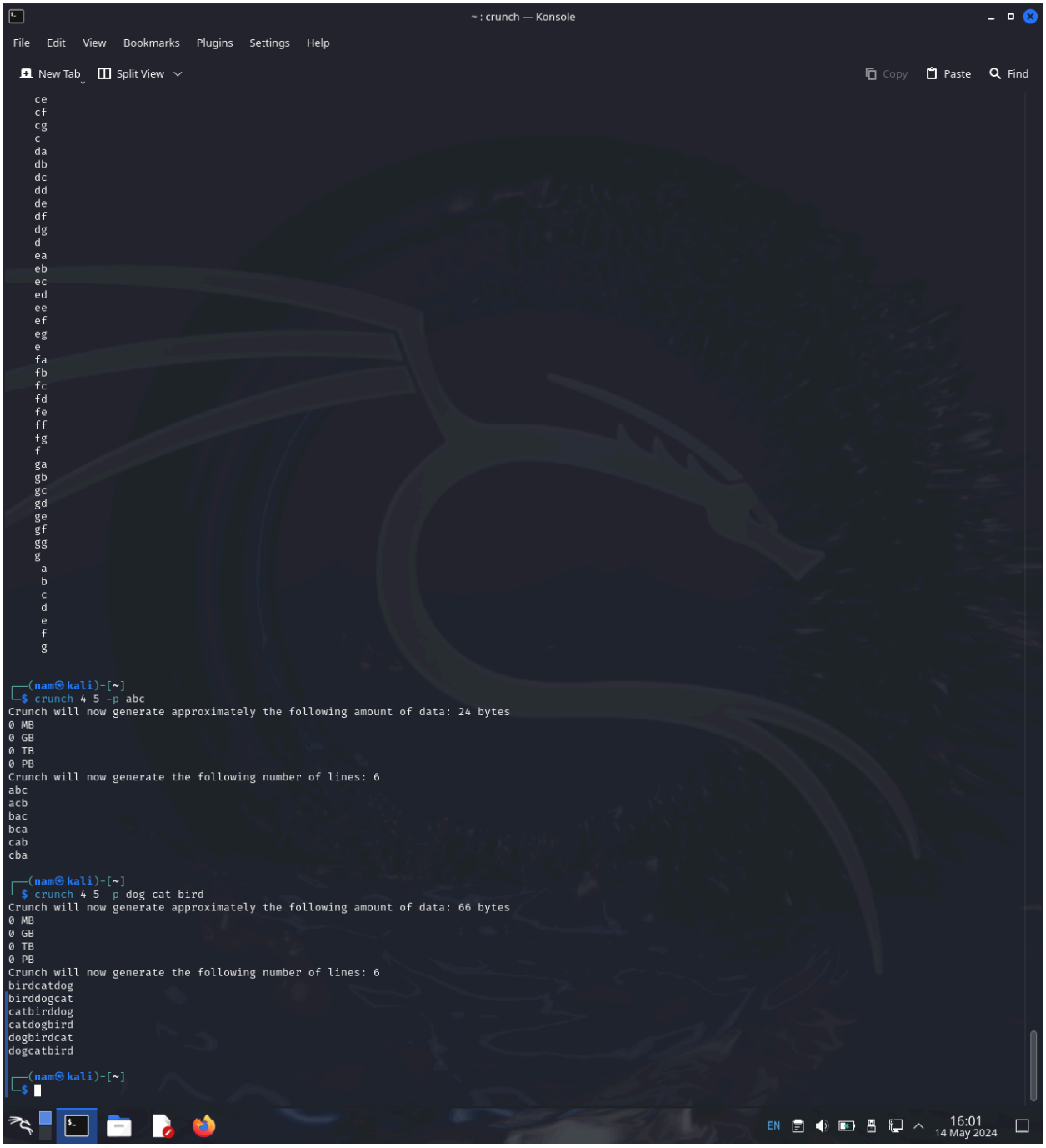

~ : man — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
CRUNCH(1) General Commands Manual CRUNCH(1)
NAME
crunch - generate wordlists from a character set
SYNOPSIS
crunch <min-len> <max-len> [<charset string>] [options]
DESCRIPTION
Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program. The required parameters are:
min-len
The minimum length string you want crunch to start at. This option is required even for parameters that won't use the value.
max-len
The maximum length string you want crunch to end at. This option is required even for parameters that won't use the value.
charset string
You may specify character sets for crunch to use on the command line or if you leave it blank crunch will use the default character sets. The order MUST BE lower case characters, upper case characters, numbers, and then symbols. If you don't follow this order you will not get the results you want. You MUST specify either values for the character type or a plus sign. NOTE: If you want to include the space character in your character set you must escape it using the \ character or enclose your character set in quotes i.e. "abc ". See the examples 3, 11, 12, and 13 for examples.
OPTIONS
-b number[type]
Specifies the size of the output file, only works if -o START is used, i.e.: 60MB The output files will be in the format of starting letter-ending letter for example: ./crunch 4 5 -b 20mib -o START will generate 4 files: aaaa-gvfed.txt, gvfee-ombqy.txt, ombqz-wcydt.txt, wcydu-zzzzz.txt valid values for type are kb, mb, gb, kib, mib, and gib. The first three types are based on 1000 while the last three types are based on 1024. NOTE There is no space between the number and type. For example 500mb is correct 500 mb is NOT correct.
-c number
Specifies the number of lines to write to output file, only works if -o START is used, i.e.: 60 The output files will be in the format of starting letter-ending letter for example: ./crunch 1 1 -f /pentest/password/crunch/charset.lst mixalpha-numeric-all-space -o START -c 60 will result in 2 files: a-7.txt and 8-\ .txt The reason for the slash in the second filename is the ending character is space and ls has to escape it to print it. Yes you will need to put in the \ when specifying the filename because the last character is a space.
-d numbersymbol
Limits the number of duplicate characters. -d 2@ limits the lower case alphabet to output like aab and aac. aaa would not be generated as that is 3 consecutive letters of a. The format is number then symbol where number is the maximum number of consecutive characters and symbol is the symbol of the the character set you want to limit i.e. @,%^ See examples 17-19.
-e string
Specifies when crunch should stop early
-f /path/to/charset.lst charset-name
Specifies a character set from the charset.lst
-i Inverts the output so instead of aaa,aab,aac,aad, etc you get aaa,baa,caa,daa,aba,bba, etc
-l When you use the -t option this option tells crunch which symbols should be treated as literals. This will allow you to use the placeholders as letters in the pattern. The -l option should be the same length as the -t option. See example 15.
-m Merged with -p. Please use -p instead.
-o wordlist.txt
Specifies the file to write the output to, eg: wordlist.txt
-p charset OR -p word1 word2 ...
Tells crunch to generate words that don't have repeating characters. By default crunch will generate a wordlist size of #of_chars_in_charset ^ max_length. This option will instead generate #of_chars_in_charset!. The ! stands for factorial. For example say the charset is abc and max length is 4.. Crunch will by default generate 3^4 = 81 words. This option will instead generate 3! = 3×2×1 = 6 words (abc, acb, bac, bca, cab, cba). THIS MUST BE THE LAST OPTION! This option CANNOT be used with -s and it ignores min and max length however you must still specify two numbers.
-q filename.txt
Tells crunch to read filename.txt and permute what is read. This is like the -p option except it gets the input from filename.txt.
-r Tells crunch to resume generate words from where it left off. -r only works if you use -o. You must use the same command as the original command used to generate the words. The only exception to this is the -s option. If your original command used the -s option you MUST remove it before you resume the session. Just add -r to the end of the original command.
-s startblock
Manual page crunch(1) line 1 (press h for help or q to quit)
EN
15:52
14 May 2024

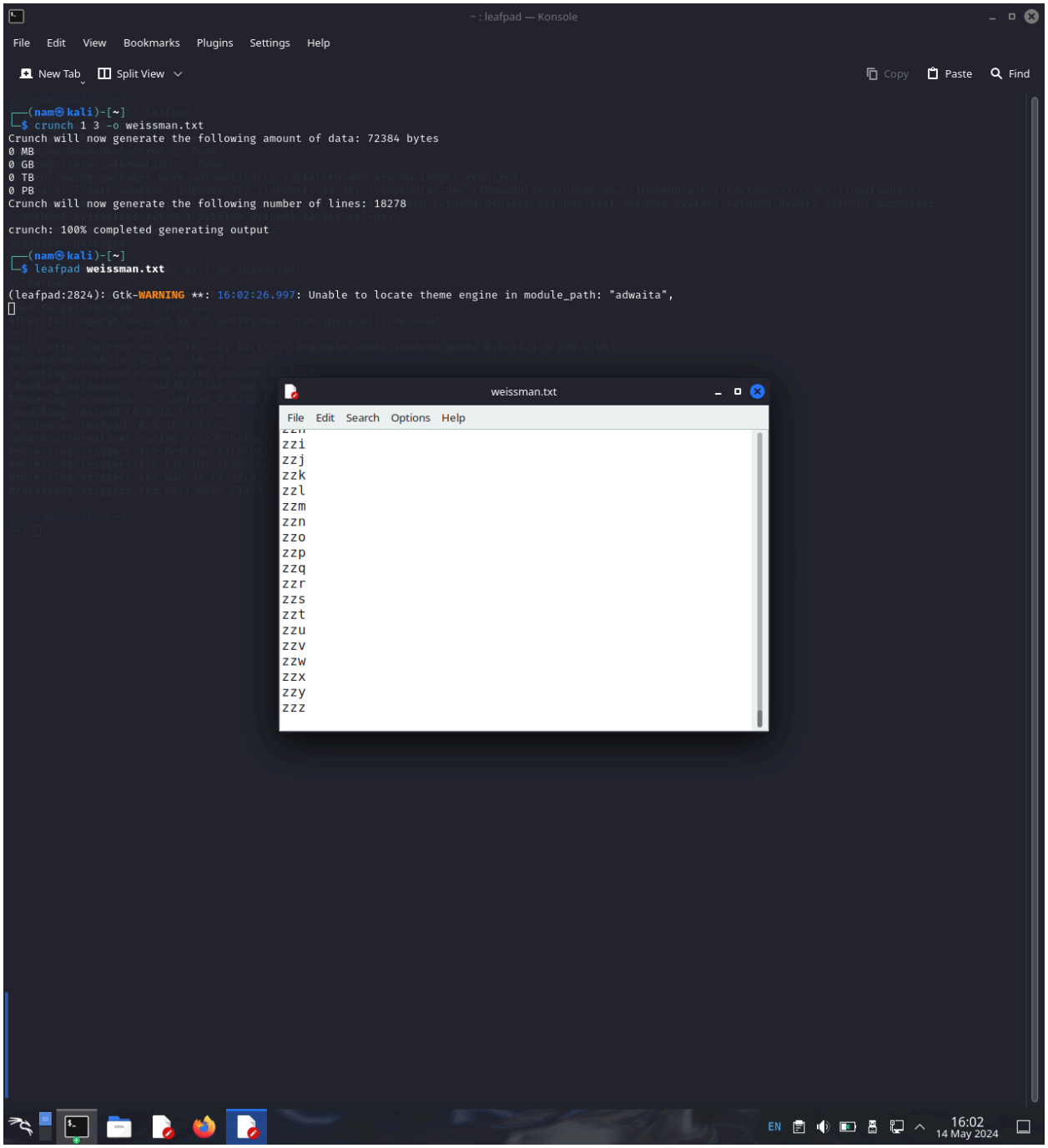

~ : crunch — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ crunch
crunch version 3.6
Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program.
Usage: crunch <min> <max> [options]
where min and max are numbers
Please refer to the man page for instructions and examples on how to use crunch.
┌──(nam㉿kali)-[~]
└─$ crunch 1 8
Crunch will now generate the following amount of data: 1945934118544 bytes
1855787 MB
1812 GB
1 TB
0 PB
Crunch will now generate the following number of lines: 217180147158
EN
15:54
14 May 2024

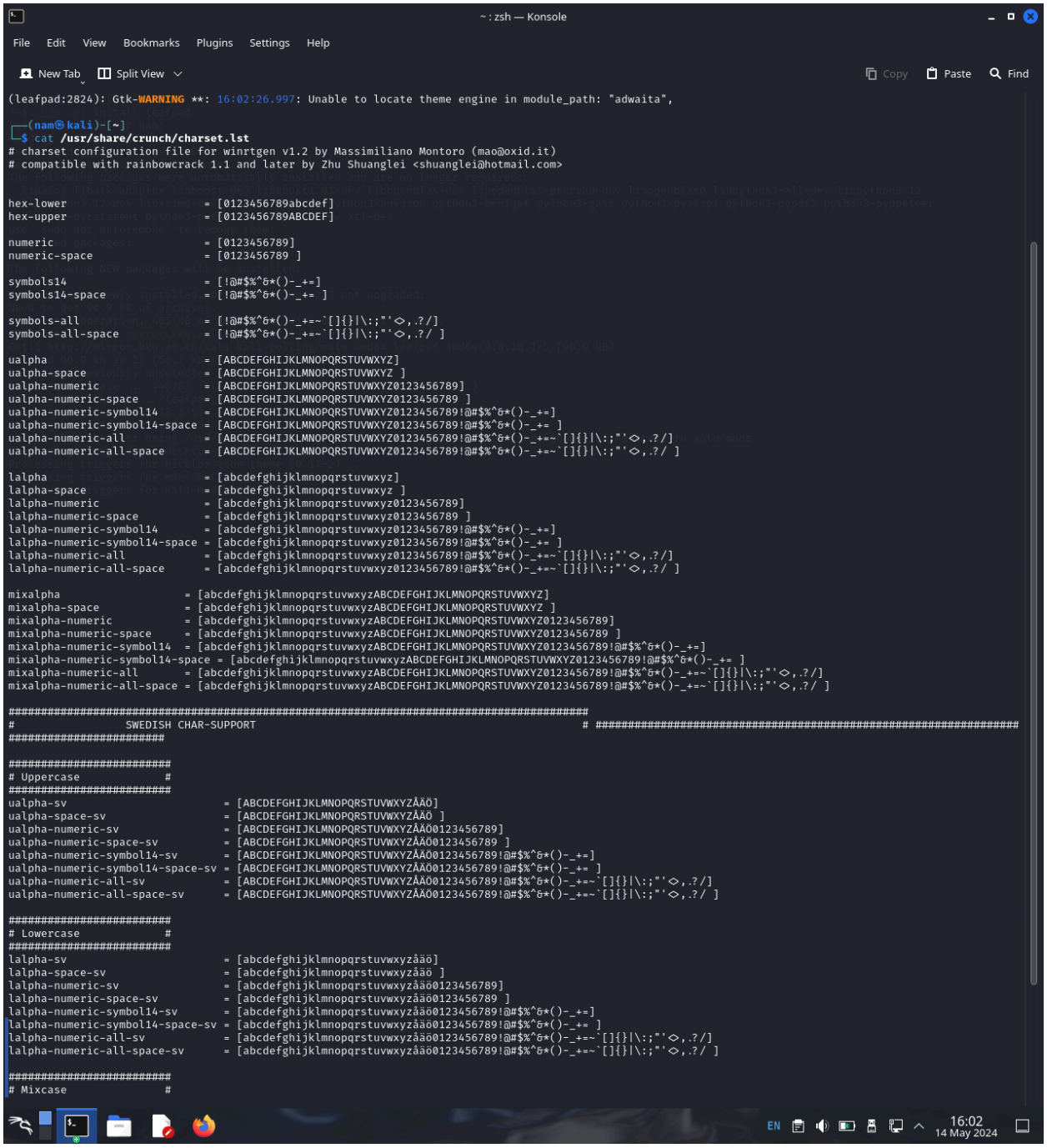

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
sunpjy
sunpjz
sunpka
sunpkb
sunpkc
sunpkd
sunpke
sunpkf
sunpkg
sunpkh
sunpki
sunpkj
sunpkk
sunpkl
sunpkm
sunpkn
sunpko
sunpkp
sunpkq
sunpkr
sunpks
sunpkt
sunpku
sunpkv
sunpkw
sunpkx
sunpky
sunpkz
sunpla
sunplb
sunplc
sunpld
sunple
sunplf
sunplg
sunplh
sunpli
sunplj
sunplk
sunpll
sunplm
sunpln
sunplo
sunplp
sunplq
sunplr
sunpls
sunplt
sunplu
sunplv
sunplw
sunplx
sunply
sunplz
sunpma
sunpmb
sunpmc
sunpmd
sunpme
sunpmf
sunpmg
sunpmh
sunpmi
sunpmj
sunpmk
sun^Csunrpy
Crunch ending at sunrpy
┌──(nam㉿kali)-[~]
└─$ crunch 1 6 abcdefg
Crunch will now generate the following amount of data: 937923 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 137256
EN
15:58
14 May 2024

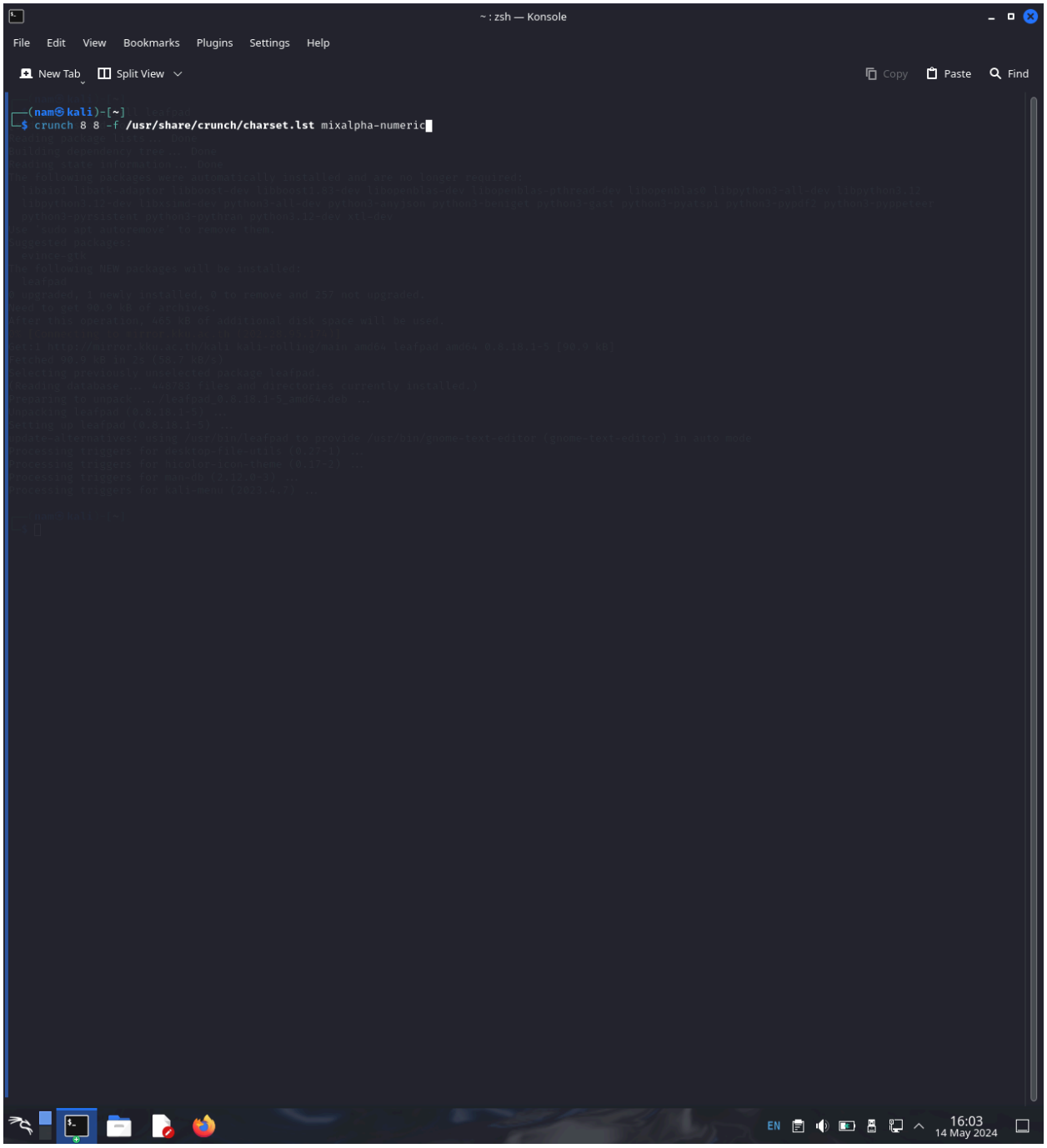

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
gggfee
gggfef
gggfeg
gggffa
gggffb
gggffc
gggffd
gggffe
gggfff
gggffg
gggfga
gggfgb
gggfgc
gggfgd
gggfge
gggfgf
gggfgg
ggggaa
ggggab
ggggac
ggggad
ggggae
ggggaf
ggggag
ggggba
ggggbb
ggggbc
ggggbd
ggggbe
ggggbf
ggggbg
ggggca
ggggcb
ggggcc
ggggcd
ggggce
ggggcf
ggggcg
ggggda
ggggdb
ggggdc
ggggdd
ggggde
ggggdf
ggggdg
ggggea
ggggeb
ggggec
gggged
ggggee
ggggef
ggggeg
ggggfa
ggggfb
ggggfc
ggggfd
ggggfe
ggggff
ggggfg
gggggа
ggggb
gggggc
ggggd
gggggе
ggggf
gggggg
┌──(nam㉿kali)-[~]
└─$ crunch 1 6 abcdefg\
>
Crunch will now generate the following amount of data: 937923 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 137256
EN
15:59
14 May 2024

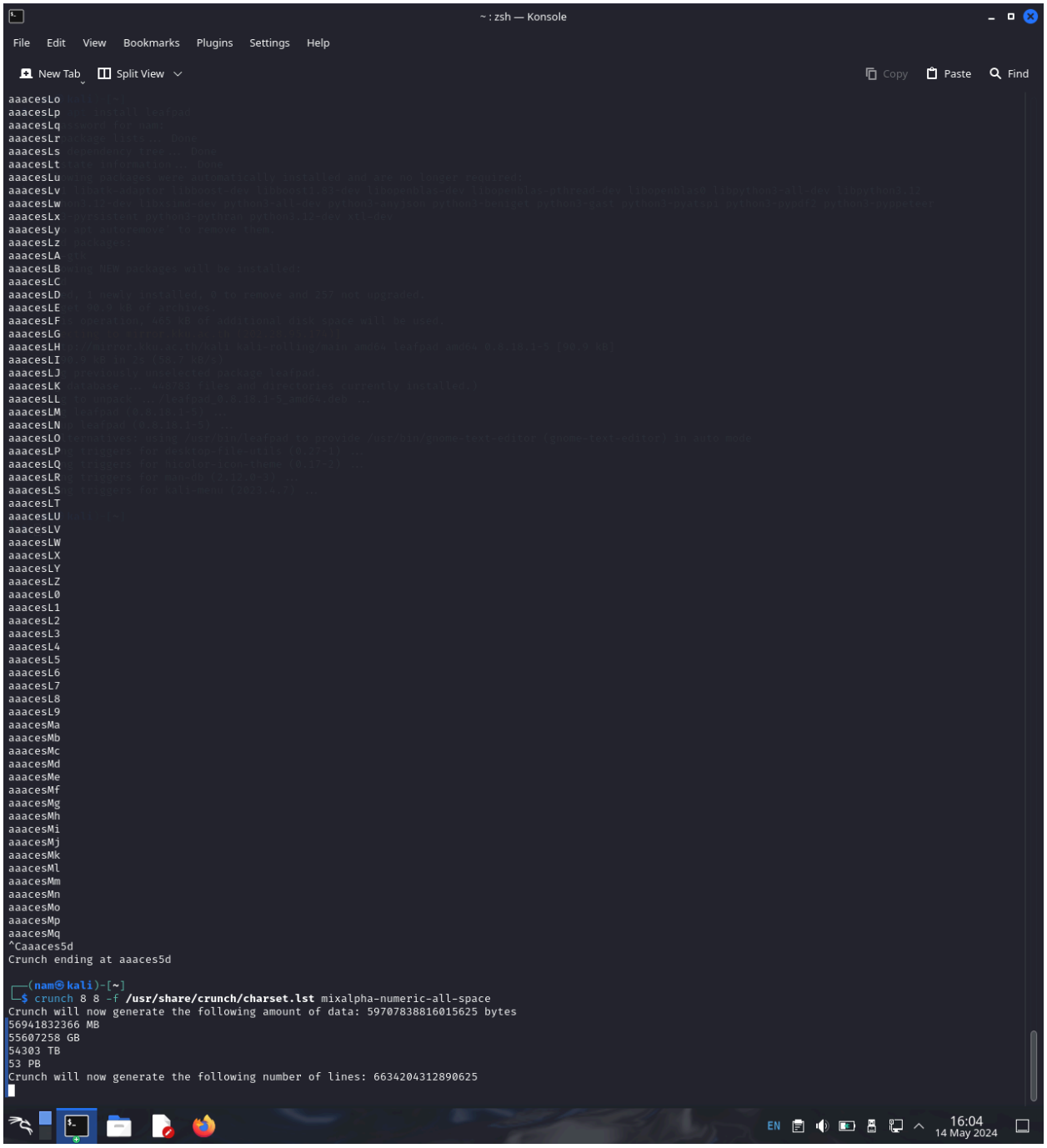

~ : crunch — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
g f
g g
g
aa
ab
ac
ad
ae
af
ag
a
ba
bb
bc
bd
be
bf
bg
b
ca
cb
cc
cd
ce
cf
cg
c
da
db
dc
dd
de
df
dg
d
ea
eb
ec
ed
ee
ef
eg
e
fa
fb
fc
fd
fe
ff
fg
f
ga
gb
gc
gd
ge
gf
gg
g
a
b
c
d
e
f
g
(nam㉿kali)-[~]
$ crunch 4 5 -p abc
Crunch will now generate approximately the following amount of data: 24 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
EN
16:00
14 May 2024

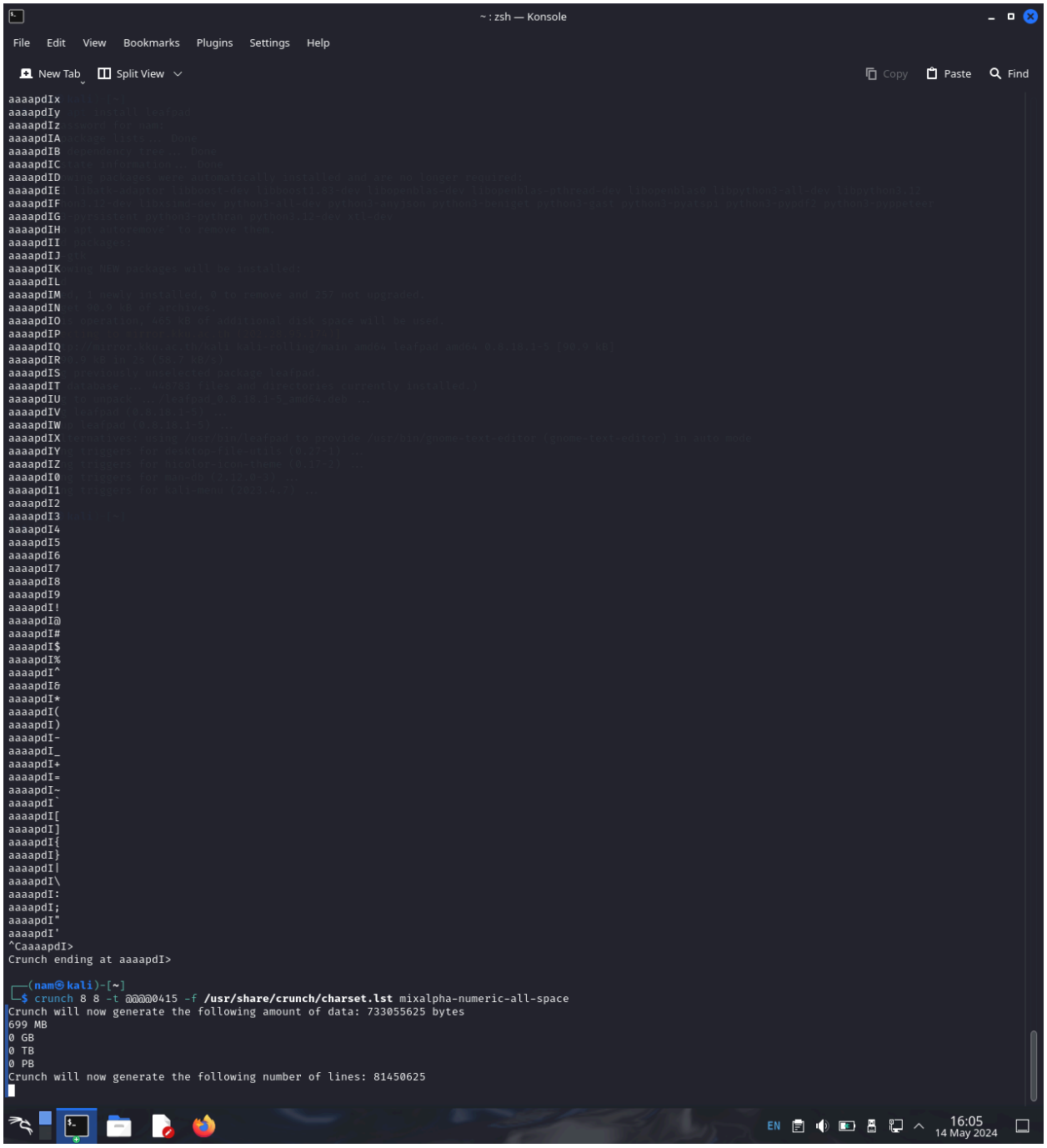

~ : crunch — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
ce
cf
cg
c
da
db
dc
dd
de
df
dg
d
ea
eb
ec
ed
ee
ef
eg
e
fa
fb
fc
fd
fe
ff
fg
f
ga
gb
gc
gd
ge
gf
gg
g
a
b
c
d
e
f
g
┌──(nam㉿kali)-[~]
└─$ crunch 4 5 -p abc
Crunch will now generate approximately the following amount of data: 24 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
abc
acb
bac
bca
cab
cba
┌──(nam㉿kali)-[~]
└─$ crunch 4 5 -p dog cat bird
Crunch will now generate approximately the following amount of data: 66 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
birdcatdog
birddogcat
catbirddog
catdogbird
dogbirdcat
dogcatbird
┌──(nam㉿kali)-[~]
└─$
EN
16:01
14 May 2024

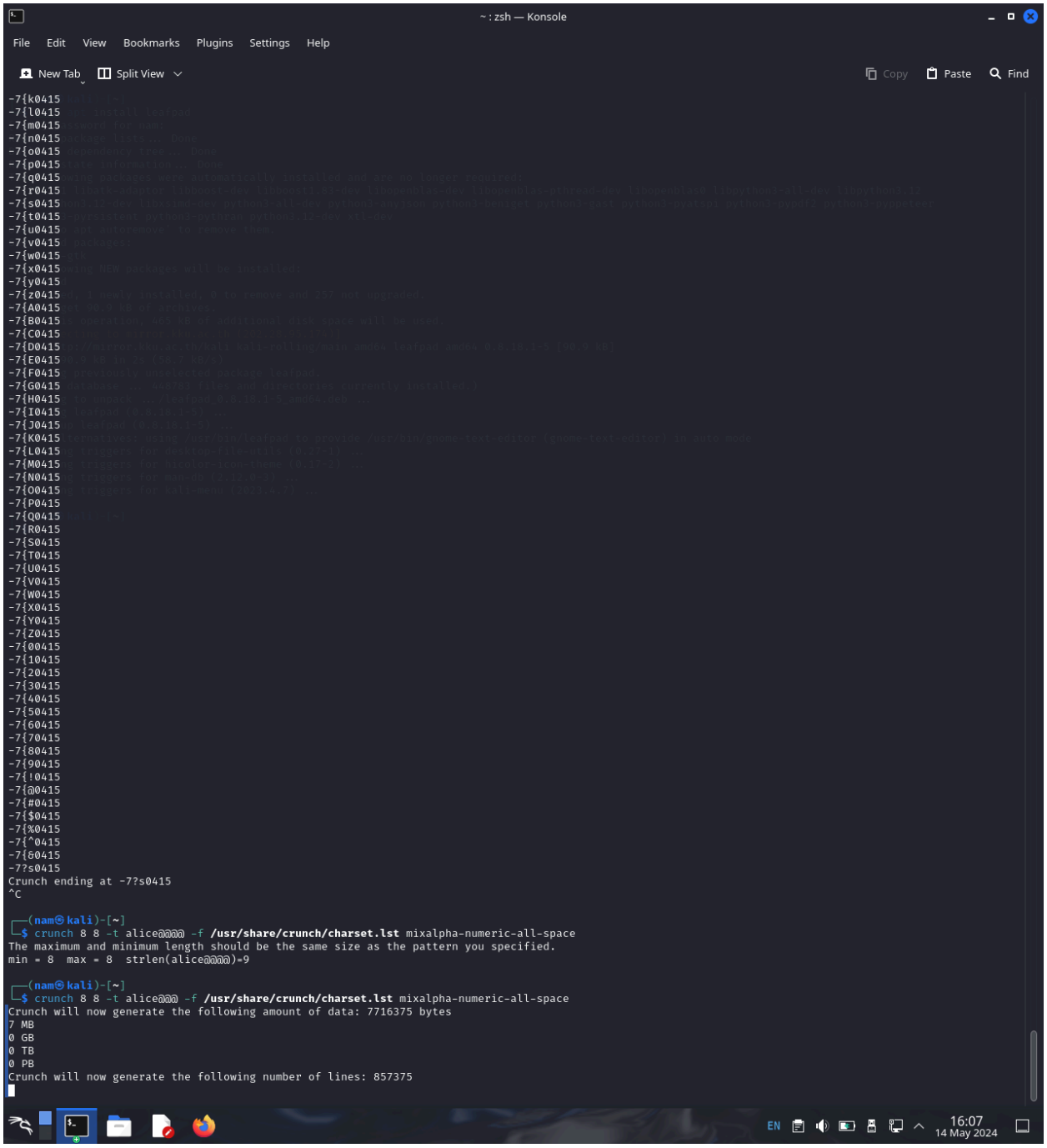

~ : leafpad — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
(nam㉿kali)-[~]
$ crunch 1 3 -o weissman.txt
Crunch will now generate the following amount of data: 72384 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 18278
crunch: 100% completed generating output
(nam㉿kali)-[~]
$ leafpad weissman.txt
(leafpad:2824): Gtk-WARNING **: 16:02:26.997: Unable to locate theme engine in module_path: "adwaita",
weissman.txt
File Edit Search Options Help
zzi
zzj
zzk
zzl
zzm
zzn
zzo
zzp
zzq
zzr
zzs
zzt
zzu
zzv
zzw
zzx
zzy
zzz
EN
16:02
14 May 2024

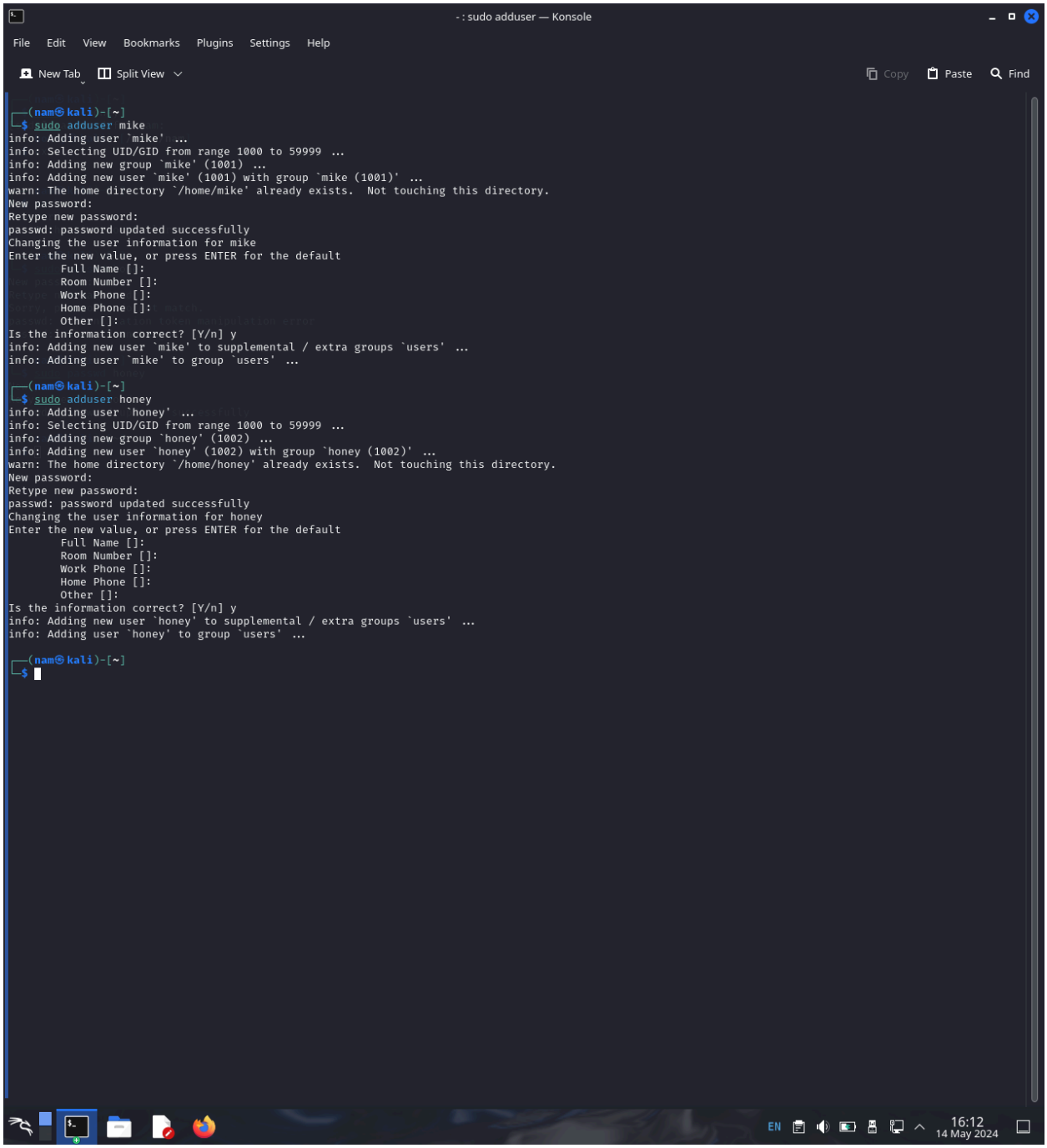

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
(leafpad:2824): Gtk-WARNING **: 16:02:26.997: Unable to locate theme engine in module_path: "adwaita",
┌──(nam㉿kali)-[~]
└─$ cat /usr/share/crunch/charset.lst
charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid.it)
compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>
hex-lower = [0123456789abcdef]
hex-upper = [0123456789ABCDEF]
numeric = [0123456789]
numeric-space = [0123456789]
symbols14 = [!@#$%^&*()-_+=]
symbols14-space = [!@#$%^&*()-_+=]
symbols-all = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
symbols-all-space = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
ualpha-numeric-symbol14-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
ualpha-numeric-all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha-numeric-all-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
lalpha = [abcdefghijklmnopqrstuvwxyz]
lalpha-space = [abcdefghijklmnopqrstuvwxyz]
lalpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]
lalpha-numeric-space = [abcdefghijklmnopqrstuvwxyz0123456789]
lalpha-numeric-symbol14 = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=]
lalpha-numeric-symbol14-space = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=]
lalpha-numeric-all = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
lalpha-numeric-all-space = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
mixalpha = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mixalpha-space = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mixalpha-numeric = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
mixalpha-numeric-space = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
mixalpha-numeric-symbol14 = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
mixalpha-numeric-symbol14-space = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
mixalpha-numeric-all = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
mixalpha-numeric-all-space = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
SWEDISH CHAR-SUPPORT
Uppercase
ualpha-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ]
ualpha-space-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ]
ualpha-numeric-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ0123456789]
ualpha-numeric-space-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ0123456789]
ualpha-numeric-symbol14-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ0123456789!@#$%^&*()-_+=]
ualpha-numeric-symbol14-space-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ0123456789!@#$%^&*()-_+=]
ualpha-numeric-all-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha-numeric-all-space-sv = [ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
Lowercase
lalpha-sv = [abcdefghijklmnopqrstuvwxyzåäö]
lalpha-space-sv = [abcdefghijklmnopqrstuvwxyzåäö]
lalpha-numeric-sv = [abcdefghijklmnopqrstuvwxyzåäö0123456789]
lalpha-numeric-space-sv = [abcdefghijklmnopqrstuvwxyzåäö0123456789]
lalpha-numeric-symbol14-sv = [abcdefghijklmnopqrstuvwxyzåäö0123456789!@#$%^&*()-_+=]
lalpha-numeric-symbol14-space-sv = [abcdefghijklmnopqrstuvwxyzåäö0123456789!@#$%^&*()-_+=]
lalpha-numeric-all-sv = [abcdefghijklmnopqrstuvwxyzåäö0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
lalpha-numeric-all-space-sv = [abcdefghijklmnopqrstuvwxyzåäö0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
Mixcase
EN
16:02
14 May 2024

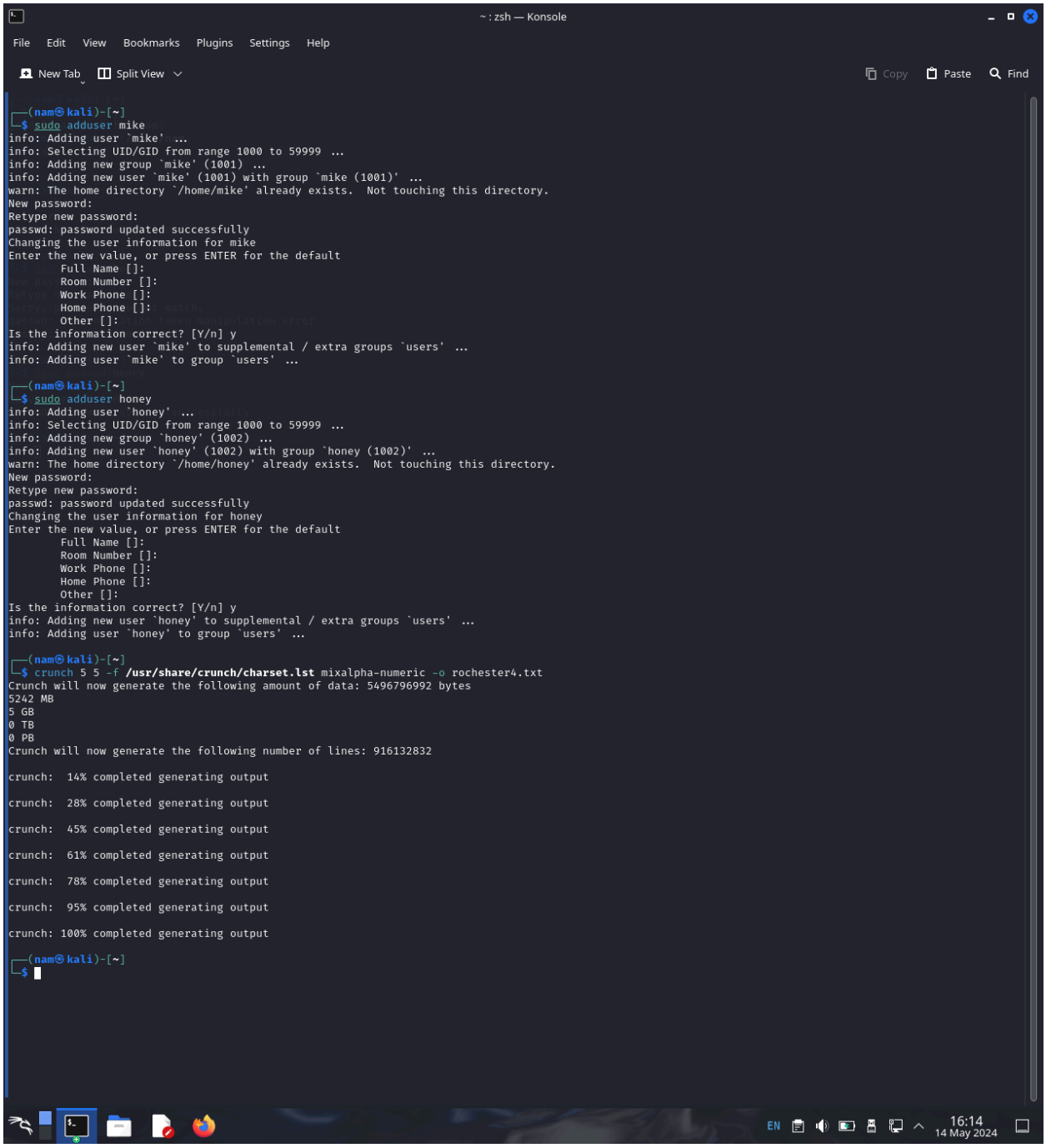

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
(nam㉿kali)-[~]
$ crunch 8 8 -f /usr/share/crunch/charset.lst mixalpha-numeric
EN
16:03
14 May 2024

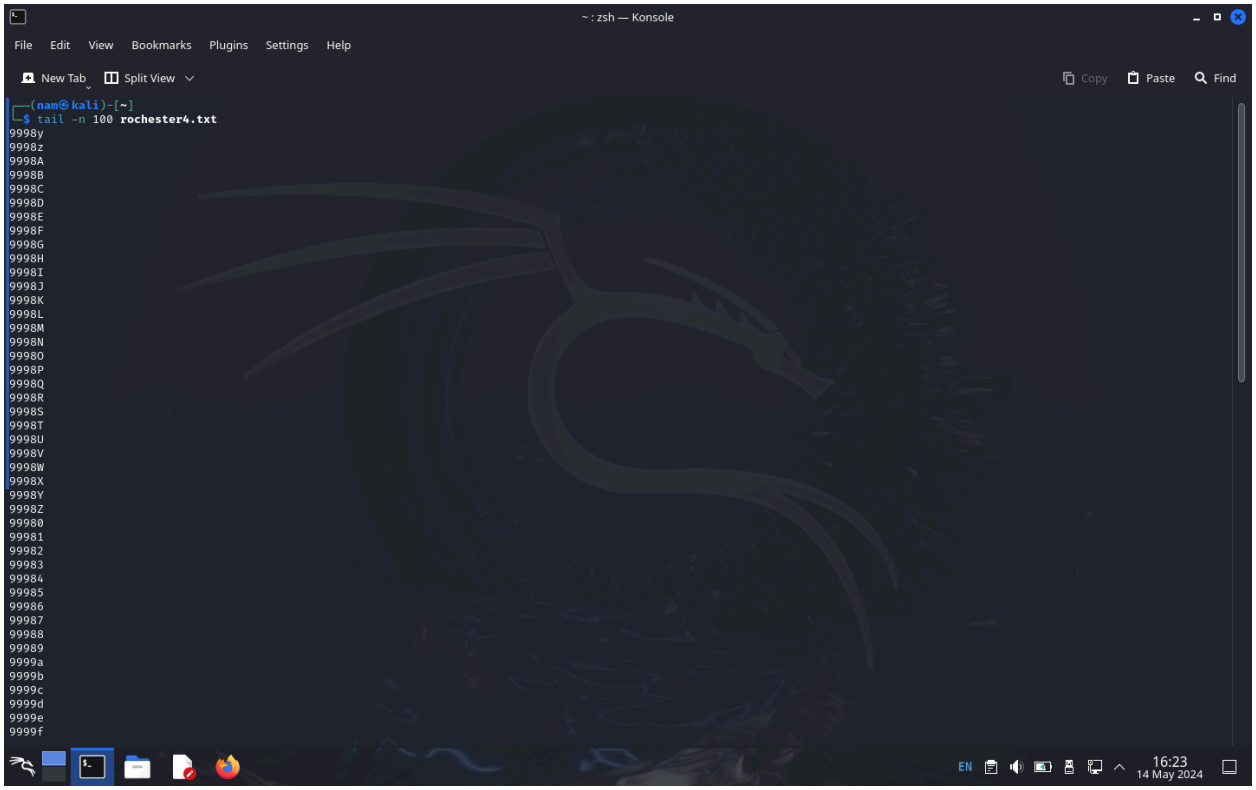

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
aaacesLo
aaacesLp
aaacesLq
aaacesLr
aaacesLs
aaacesLt
aaacesLu
aaacesLv
aaacesLw
aaacesLx
aaacesLy
aaacesLz
aaacesLA
aaacesLB
aaacesLC
aaacesLD
aaacesLE
aaacesLF
aaacesLG
aaacesLH
aaacesLI
aaacesLJ
aaacesLK
aaacesLL
aaacesLM
aaacesLN
aaacesLO
aaacesLP
aaacesLQ
aaacesLR
aaacesLS
aaacesLT
aaacesLU
aaacesLV
aaacesLW
aaacesLX
aaacesLY
aaacesLZ
aaacesL0
aaacesL1
aaacesL2
aaacesL3
aaacesL4
aaacesL5
aaacesL6
aaacesL7
aaacesL8
aaacesL9
aaacesMa
aaacesMb
aaacesMc
aaacesMd
aaacesMe
aaacesMf
aaacesMg
aaacesMh
aaacesMi
aaacesMj
aaacesMk
aaacesMl
aaacesMm
aaacesMn
aaacesMo
aaacesMp
aaacesMq
^Caaaces5d
Crunch ending at aaaces5d
┌──(nam㉿kali)-[~]
└─$ crunch 8 8 -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space
Crunch will now generate the following amount of data: 59707838816015625 bytes
56941832366 MB
55607258 GB
54303 TB
53 PB
Crunch will now generate the following number of lines: 6634204312890625
EN
16:04
14 May 2024


~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
aaaapdIx
aaaapdIy
aaaapdIz
aaaapdIA
aaaapdIB
aaaapdIC
aaaapdID
aaaapdIE
aaaapdIF
aaaapdIG
aaaapdIH
aaaapdII
aaaapdIJ
aaaapdIK
aaaapdIL
aaaapdIM
aaaapdIN
aaaapdIO
aaaapdIP
aaaapdIQ
aaaapdIR
aaaapdIS
aaaapdIT
aaaapdIU
aaaapdIV
aaaapdIW
aaaapdIX
aaaapdIY
aaaapdIZ
aaaapdI0
aaaapdI1
aaaapdI2
aaaapdI3
aaaapdI4
aaaapdI5
aaaapdI6
aaaapdI7
aaaapdI8
aaaapdI9
aaaapdI!
aaaapdI@
aaaapdI#
aaaapdI$
aaaapdI%
aaaapdI^
aaaapdI&
aaaapdI*
aaaapdI(
aaaapdI)
aaaapdI-
aaaapdI_
aaaapdI+
aaaapdI=
aaaapdI~
aaaapdI`
aaaapdI[
aaaapdI]
aaaapdI{
aaaapdI}
aaaapdI|
aaaapdI\
aaaapdI:
aaaapdI;
aaaapdI"
aaaapdI'
^CaaaapdI>
Crunch ending at aaaapdI>
┌──(nam㉿kali)-[~]
└─$ crunch 8 8 -t @@@@0415 -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space
Crunch will now generate the following amount of data: 733055625 bytes
699 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 81450625
EN
16:05
14 May 2024

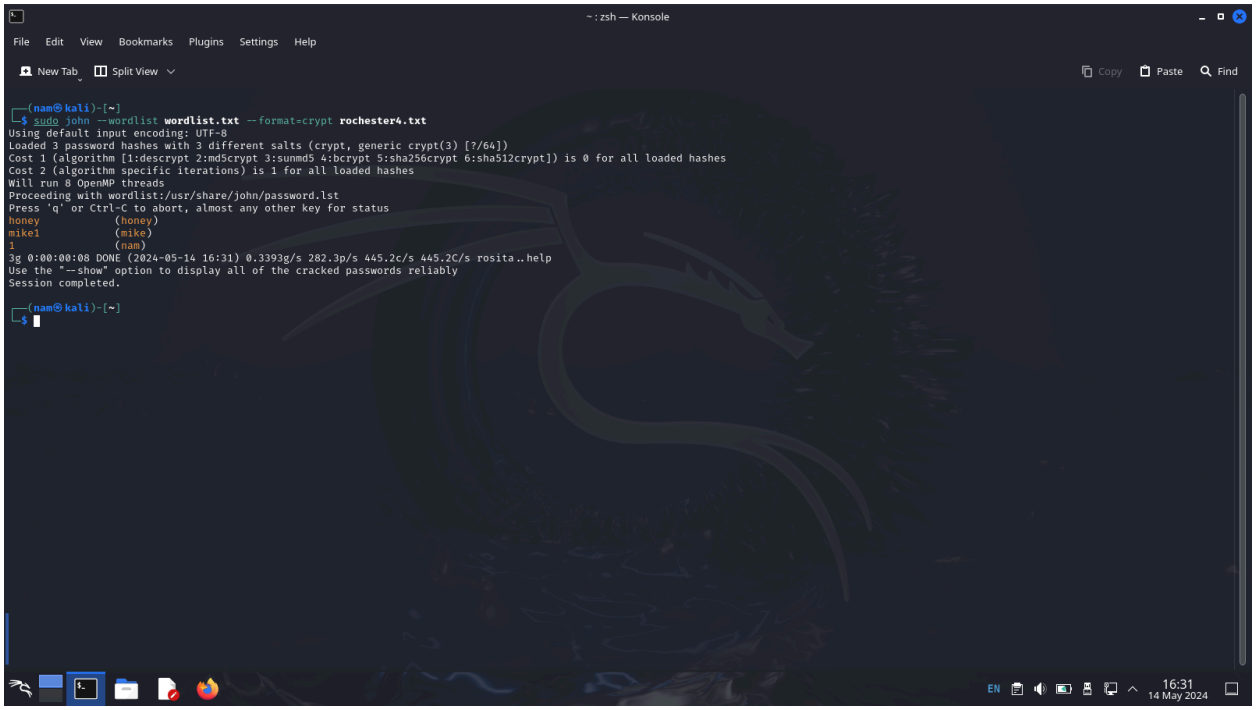

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
-7{k0415
-7{l0415
-7{m0415
-7{n0415
-7{o0415
-7{p0415
-7{q0415
-7{r0415
-7{s0415
-7{t0415
-7{u0415
-7{v0415
-7{w0415
-7{x0415
-7{y0415
-7{z0415
-7{A0415
-7{B0415
-7{C0415
-7{D0415
-7{E0415
-7{F0415
-7{G0415
-7{H0415
-7{I0415
-7{J0415
-7{K0415
-7{L0415
-7{M0415
-7{N0415
-7{O0415
-7{P0415
-7{Q0415
-7{R0415
-7{S0415
-7{T0415
-7{U0415
-7{V0415
-7{W0415
-7{X0415
-7{Y0415
-7{Z0415
-7{00415
-7{10415
-7{20415
-7{30415
-7{40415
-7{50415
-7{60415
-7{70415
-7{80415
-7{90415
-7{!0415
-7{@0415
-7{#0415
-7{$0415
-7{%0415
-7{^0415
-7{&0415
-7?s0415
Crunch ending at -7?s0415
^C
┌──(nam㉿kali)-[~]
└─$ crunch 8 8 -t alice@@@@ -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space
The maximum and minimum length should be the same size as the pattern you specified.
min = 8 max = 8 strlen(alice@@@@)=9
┌──(nam㉿kali)-[~]
└─$ crunch 8 8 -t alice@@@ -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space
Crunch will now generate the following amount of data: 7716375 bytes
7 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 857375
EN
16:07
14 May 2024

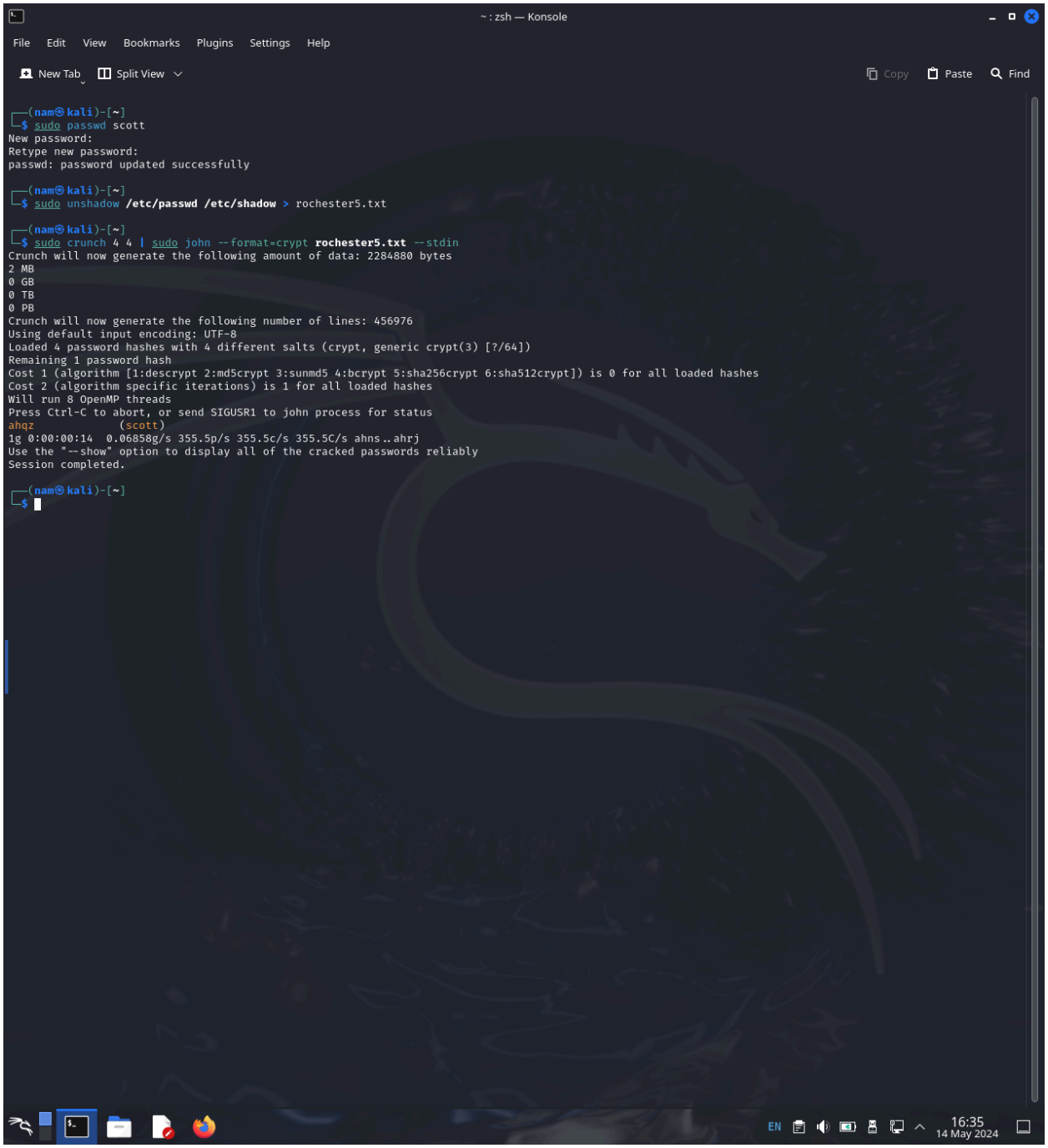

- : sudo adduser — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo adduser mike
info: Adding user `mike' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `mike' (1001) ...
info: Adding new user `mike' (1001) with group `mike (1001)' ...
warn: The home directory `/home/mike' already exists. Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mike
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
info: Adding new user `mike' to supplemental / extra groups `users' ...
info: Adding user `mike' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ sudo adduser honey
info: Adding user `honey' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `honey' (1002) ...
info: Adding new user `honey' (1002) with group `honey (1002)' ...
warn: The home directory `/home/honey' already exists. Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for honey
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
info: Adding new user `honey' to supplemental / extra groups `users' ...
info: Adding user `honey' to group `users' ...
┌──(nam㉿kali)-[~]
└─$
EN
16:12
14 May 2024

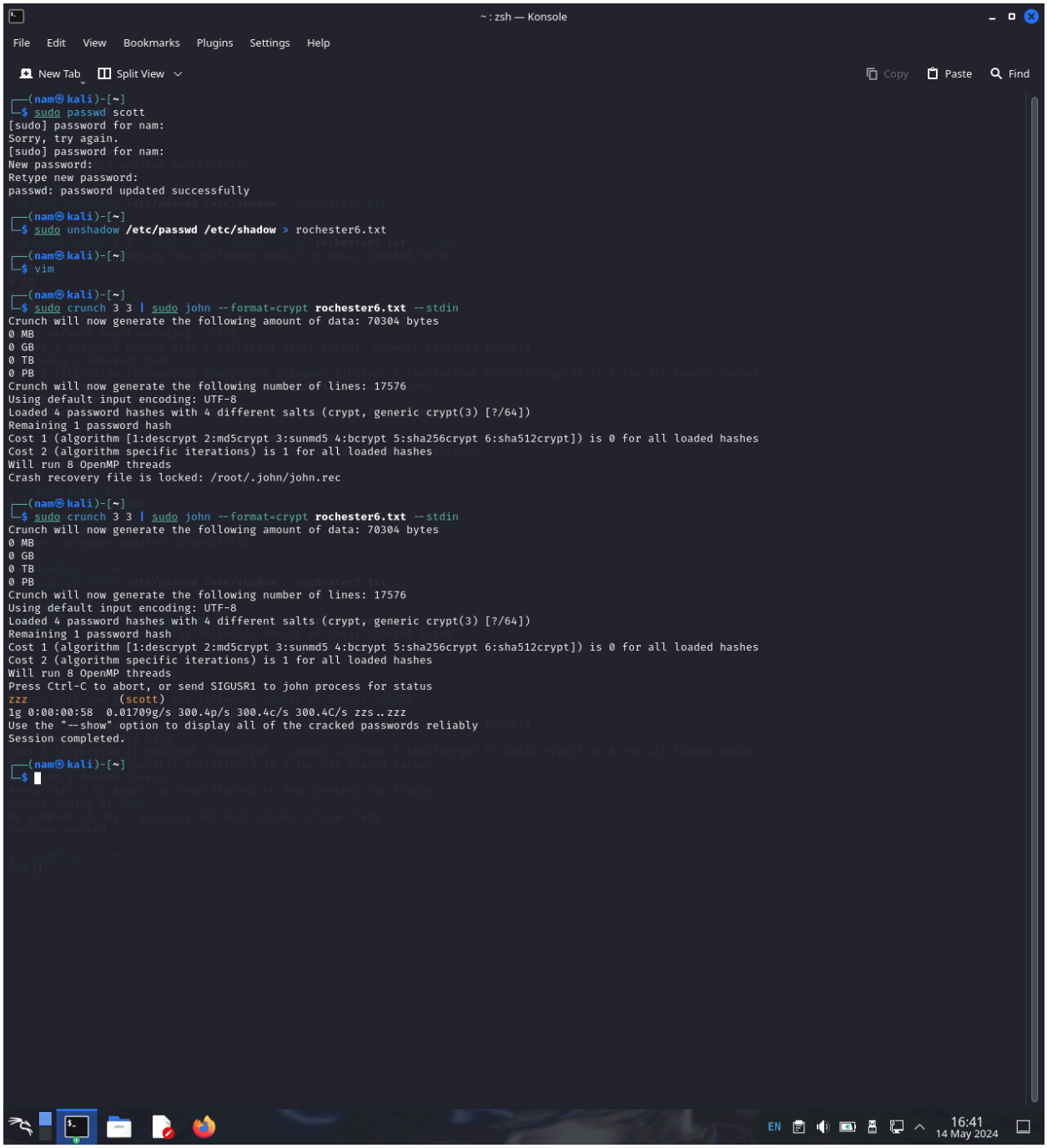

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo adduser mike
info: Adding user `mike' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `mike' (1001) ...
info: Adding new user `mike' (1001) with group `mike (1001)' ...
warn: The home directory `/home/mike' already exists. Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mike
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
info: Adding new user `mike' to supplemental / extra groups `users' ...
info: Adding user `mike' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ sudo adduser honey
info: Adding user `honey' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `honey' (1002) ...
info: Adding new user `honey' (1002) with group `honey (1002)' ...
warn: The home directory `/home/honey' already exists. Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for honey
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
info: Adding new user `honey' to supplemental / extra groups `users' ...
info: Adding user `honey' to group `users' ...
┌──(nam㉿kali)-[~]
└─$ crunch 5 5 -f /usr/share/crunch/charset.lst mixalpha-numeric -o rochester4.txt
Crunch will now generate the following amount of data: 5496796992 bytes
5242 MB
5 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 916132832
crunch: 14% completed generating output
crunch: 28% completed generating output
crunch: 45% completed generating output
crunch: 61% completed generating output
crunch: 78% completed generating output
crunch: 95% completed generating output
crunch: 100% completed generating output
┌──(nam㉿kali)-[~]
└─$
EN
16:14
14 May 2024


~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ tail -n 100 rochester4.txt
9998y
9998z
9998A
9998B
9998C
9998D
9998E
9998F
9998G
9998H
9998I
9998J
9998K
9998L
9998M
9998N
9998O
9998P
9998Q
9998R
9998S
9998T
9998U
9998V
9998W
9998X
9998Y
9998Z
99980
99981
99982
99983
99984
99985
99986
99987
99988
99989
9999a
9999b
9999c
9999d
9999e
9999f
EN
16:23
14 May 2024

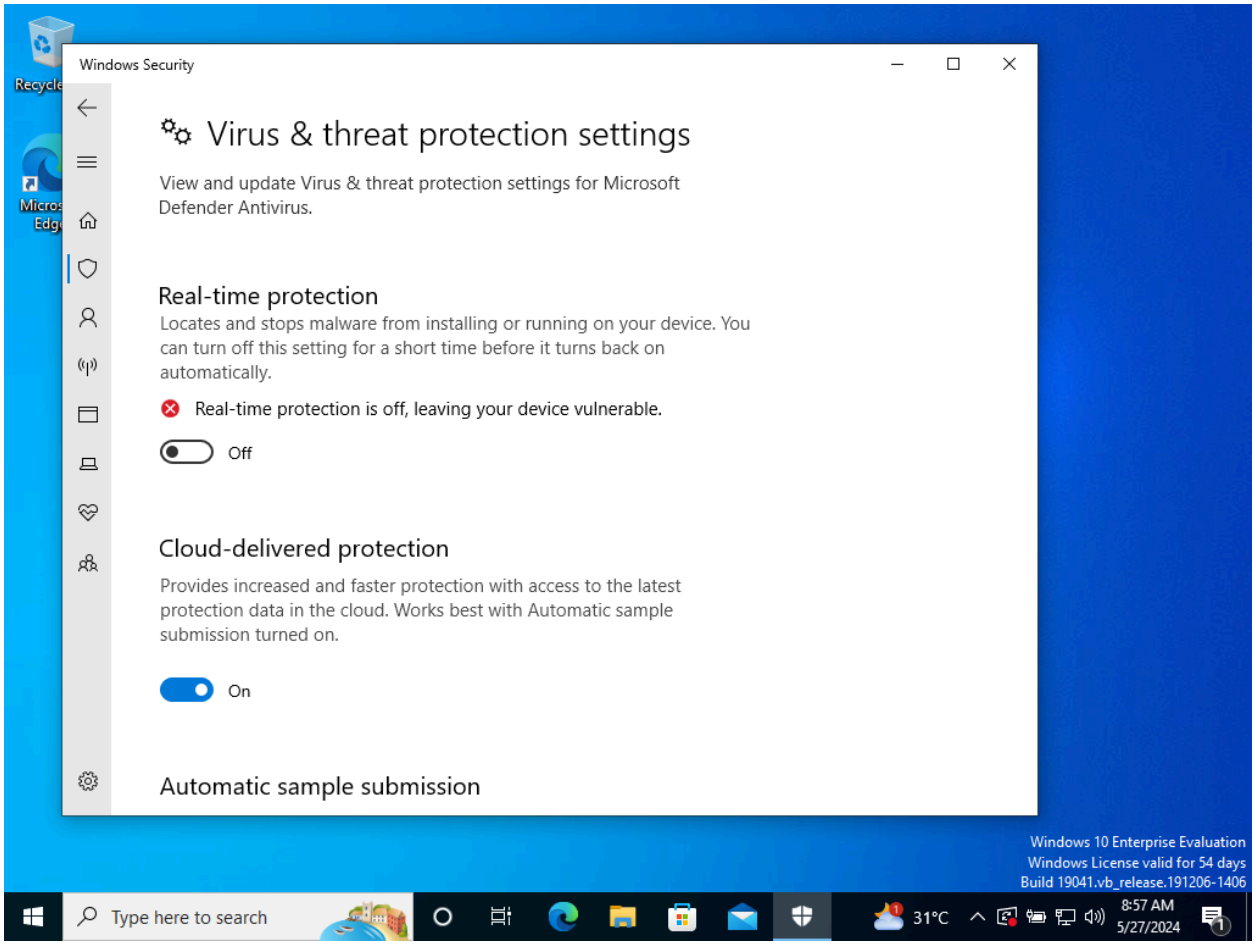

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
└─$ crunch 5 5 -f /usr/share/crunch/charset.lst mixalpha-numeric -o wordlist.txt
Crunch will now generate the following amount of data: 5496796992 bytes
5242 MB
5 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 916132832
crunch: 14% completed generating output
crunch: 23% completed generating output
crunch: 27% completed generating output
crunch: 27% completed generating output
crunch: 27% completed generating output
crunch: 27% completed generating output
crunch: 27% completed generating output
a
crunch: 31% completed generating output
crunch: 45% completed generating output
crunch: 63% completed generating output
crunch: 81% completed generating output
crunch: 99% completed generating output
crunch: 100% completed generating output
┌──(nam㉿kali)-[~]
└─$ unshadow /etc/passwd /etc/shadow > rochester4.txt
Created directory: /home/nam/.john
fopen: /etc/shadow: Permission denied
┌──(nam㉿kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > rochester4.txt
[sudo] password for nam:
Created directory: /root/.john
┌──(nam㉿kali)-[~]
└─$
EN
16:30
14 May 2024

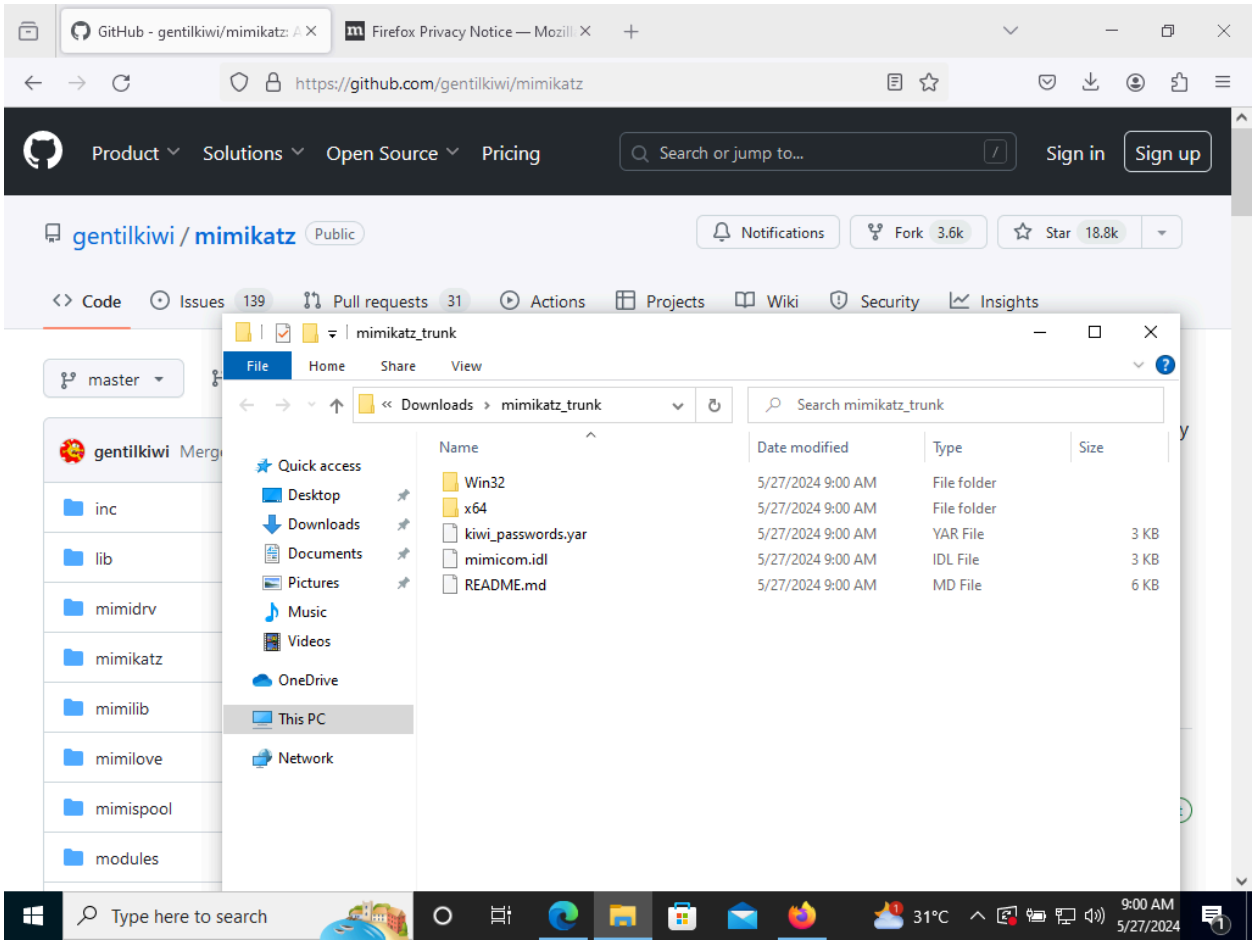

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo john --wordlist wordlist.txt --format=crypt rochester4.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
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 8 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
honey (honey)
mike1 (mike)
1 (nam)
3g 0:00:00:08 DONE (2024-05-14 16:31) 0.3393g/s 282.3p/s 445.2c/s 445.2C/s rosita..help
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(nam㉿kali)-[~]
└─$
EN
16:31
14 May 2024

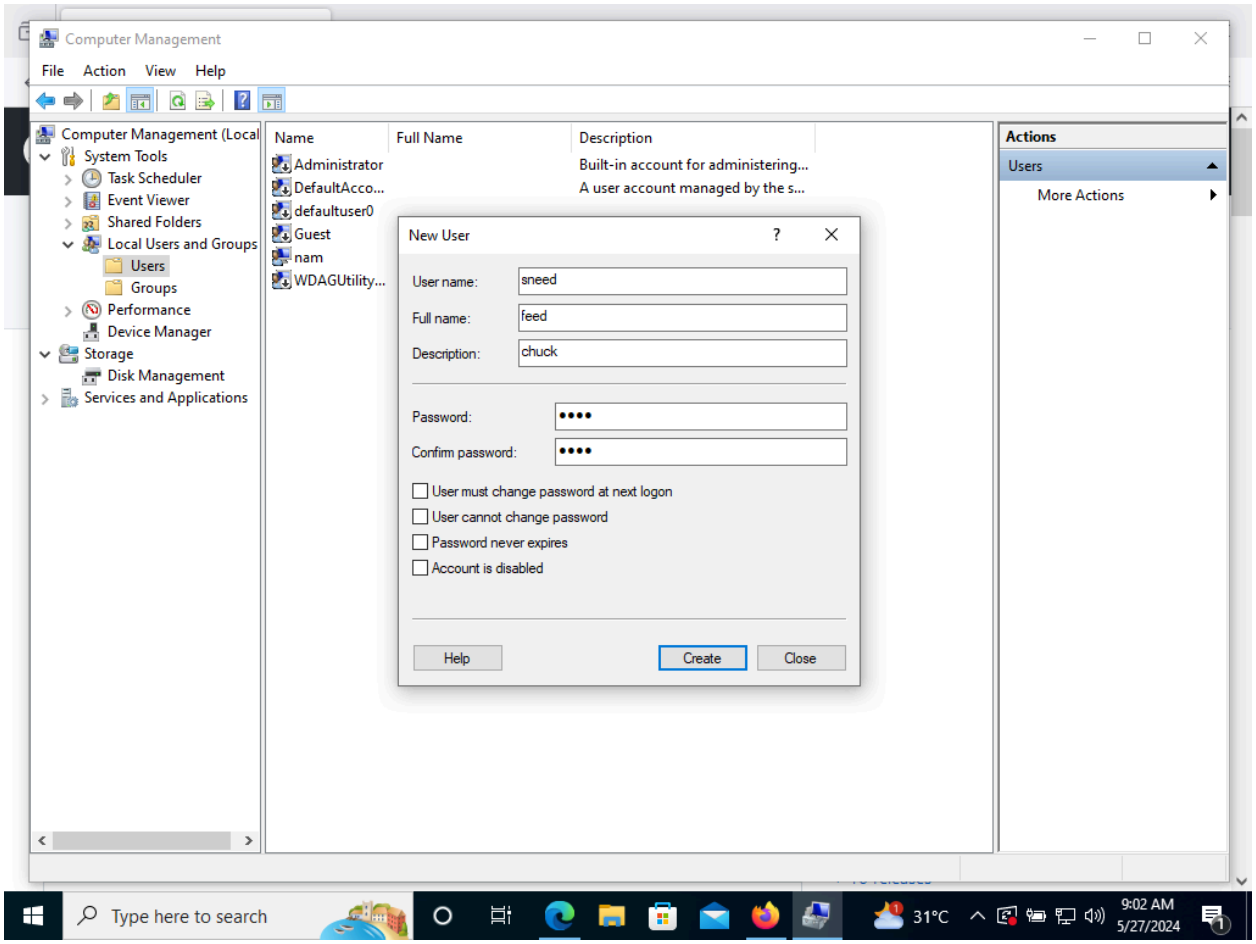

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo passwd scott
New password:
Retype new password:
passwd: password updated successfully
┌──(nam㉿kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > rochester5.txt
┌──(nam㉿kali)-[~]
└─$ sudo crunch 4 4 | sudo john --format=crypt rochester5.txt --stdin
Crunch will now generate the following amount of data: 2284880 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 456976
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
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 8 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
ahqz (scott)
1g 0:00:00:14 0.06858g/s 355.5p/s 355.5c/s 355.5C/s ahns..ahrj
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(nam㉿kali)-[~]
└─$
EN
16:35
14 May 2024

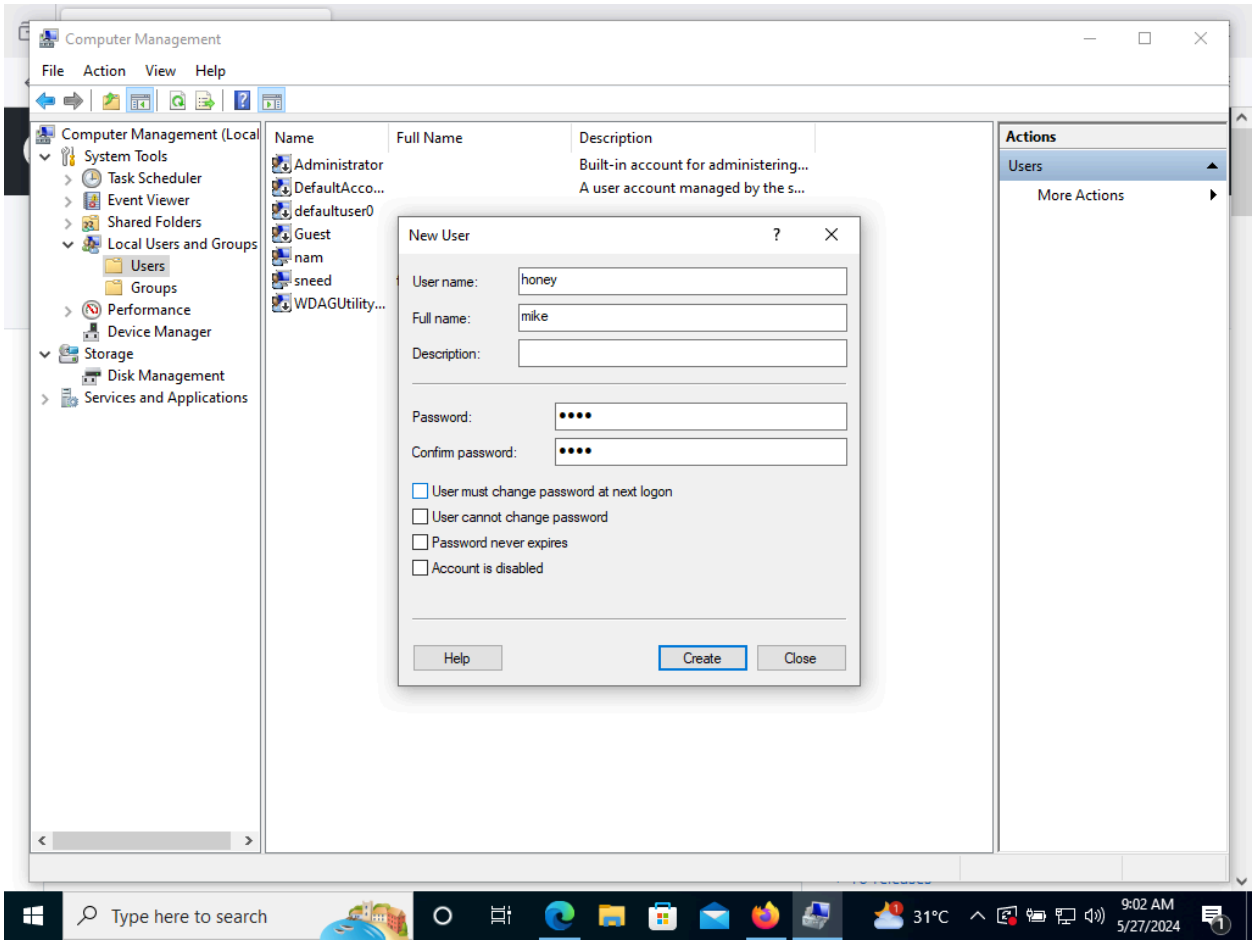

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo passwd scott
[sudo] password for nam:
Sorry, try again.
[sudo] password for nam:
New password:
Retype new password:
passwd: password updated successfully
┌──(nam㉿kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > rochester6.txt
┌──(nam㉿kali)-[~]
└─$ vim
┌──(nam㉿kali)-[~]
└─$ sudo crunch 3 3 | sudo john --format=crypt rochester6.txt --stdin
Crunch will now generate the following amount of data: 70304 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 17576
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
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 8 OpenMP threads
Crash recovery file is locked: /root/.john/john.rec
┌──(nam㉿kali)-[~]
└─$ sudo crunch 3 3 | sudo john --format=crypt rochester6.txt --stdin
Crunch will now generate the following amount of data: 70304 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 17576
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
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 8 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
zzz (scott)
1g 0:00:00:58 0.01709g/s 300.4p/s 300.4c/s 300.4C/s zzs..zzz
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(nam㉿kali)-[~]
└─$
EN
16:41
14 May 2024

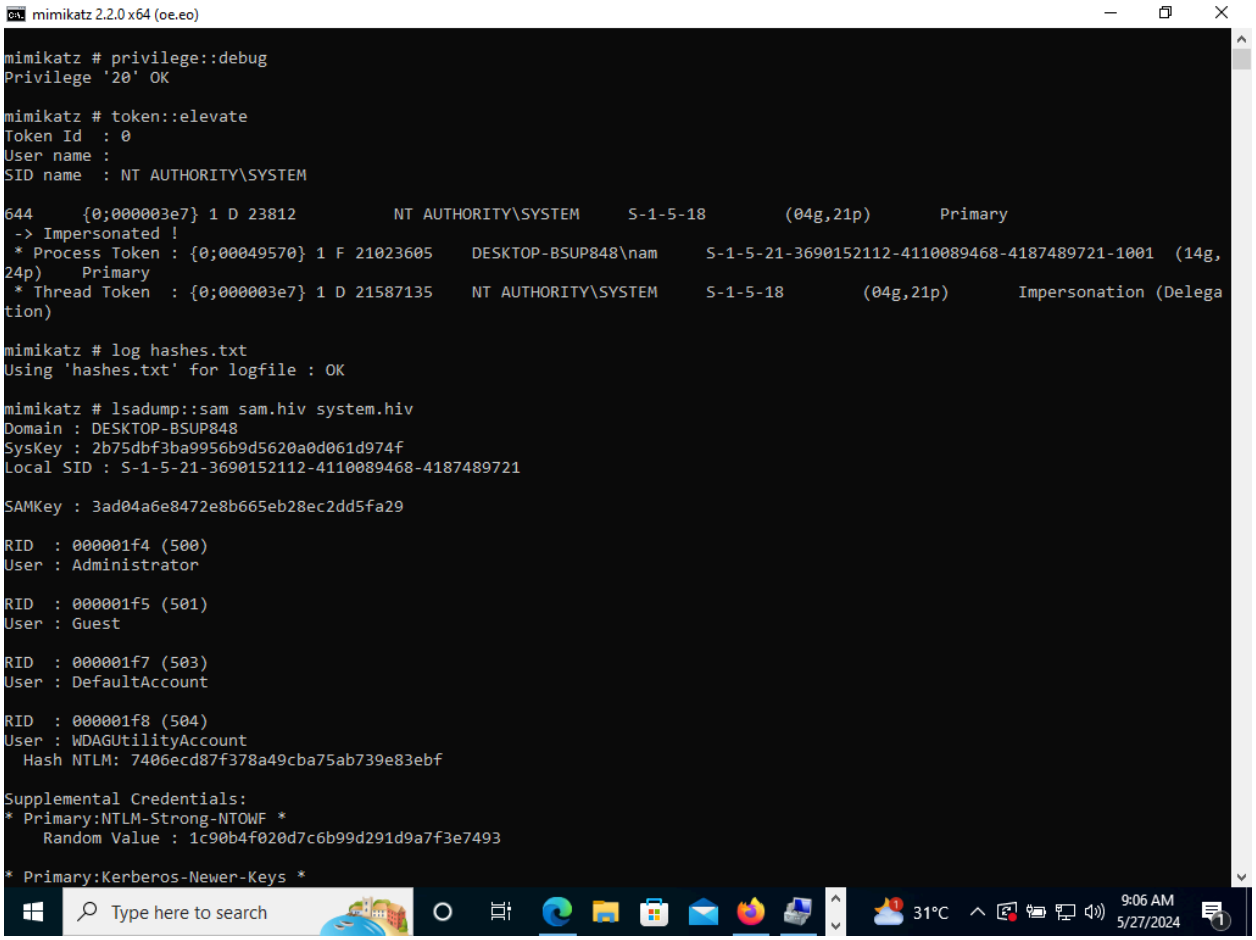
11.03

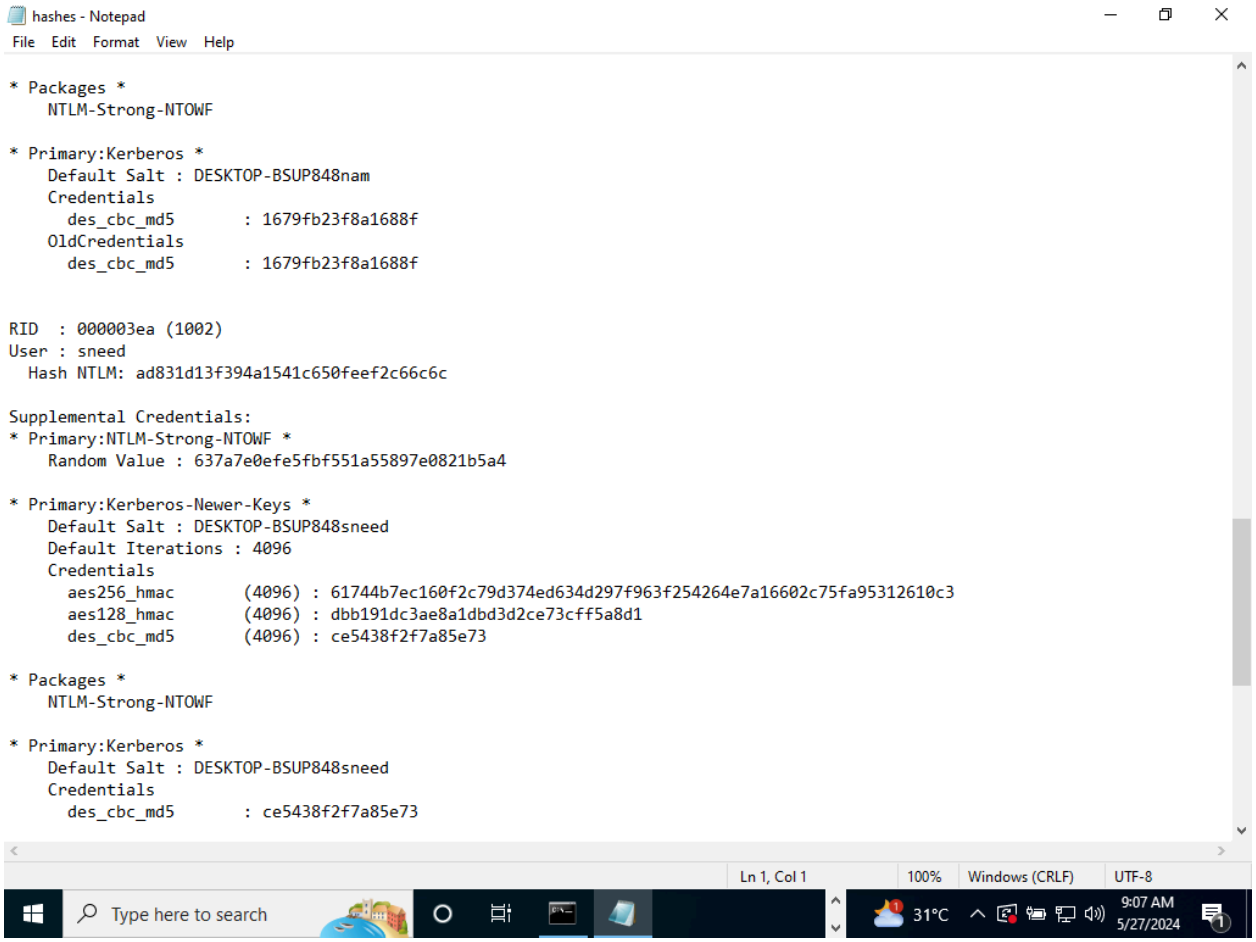

Windows Security
Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
Real-time protection is off, leaving your device vulnerable.
Off
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
Automatic sample submission
Windows 10 Enterprise Evaluation
Windows License valid for 54 days
Build 19041.vb_release.191206-1406
Type here to search
31°C
8:57 AM
5/27/2024

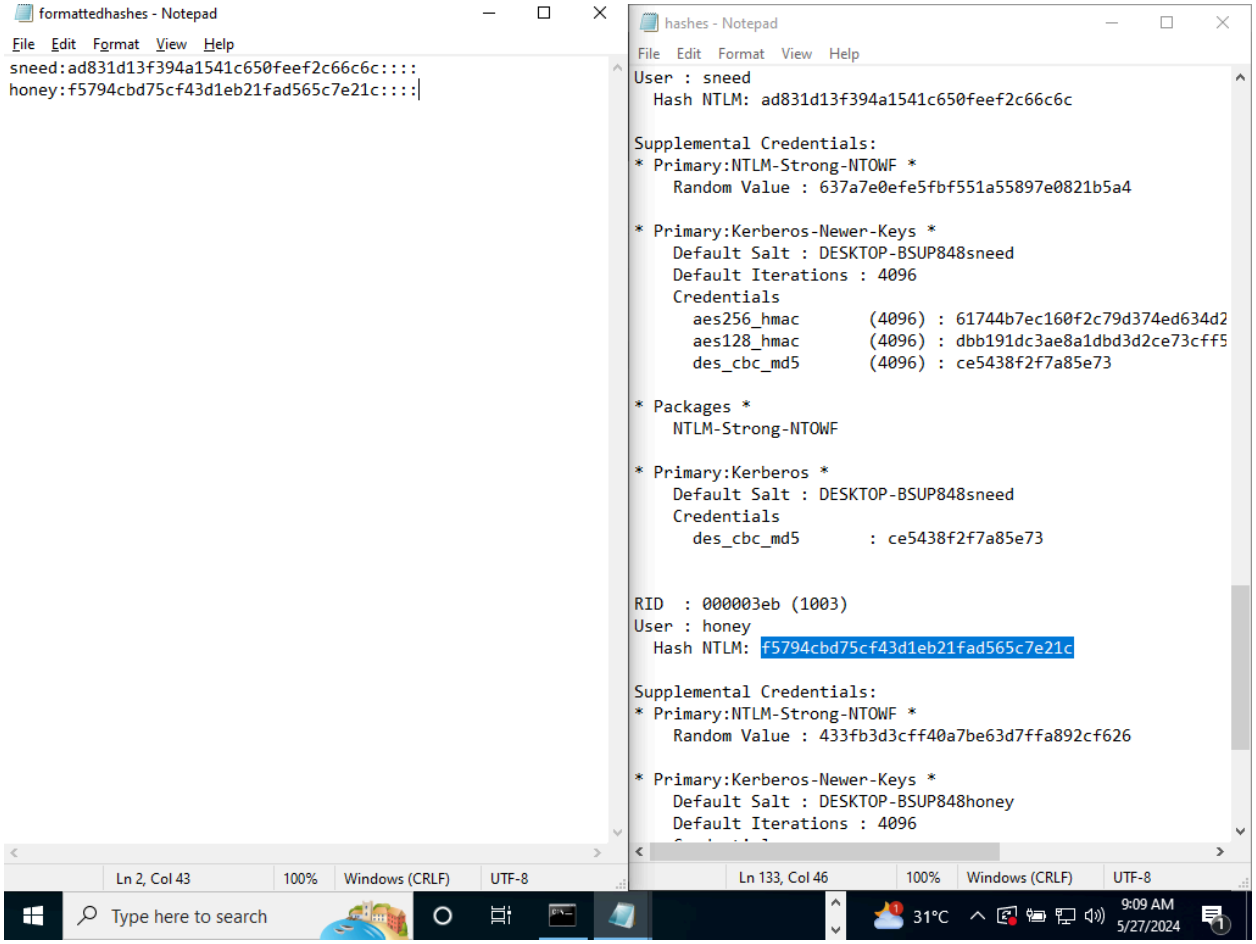

GitHub - gentilkiwi/mimikatz
Firefox Privacy Notice — Mozill
https://github.com/gentilkiwi/mimikatz
Product
Solutions
Open Source
Pricing
Search or jump to...
Sign in
Sign up
gentilkiwi / mimikatz
Public
Notifications
Fork 3.6k
Star 18.8k
Code
Issues 139
Pull requests 31
Actions
Projects
Wiki
Security
Insights
master
gentilkiwi
inc
lib
mimidrv
mimikatz
mimilib
mimilove
mimispool
modules
mimikatz_trunk
File
Home
Share
View
Downloads › mimikatz_trunk
Search mimikatz_trunk
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Win32
5/27/2024 9:00 AM
File folder
x64
5/27/2024 9:00 AM
File folder
kiwi_passwords.yar
5/27/2024 9:00 AM
YAR File
3 KB
mimicom.idl
5/27/2024 9:00 AM
IDL File
3 KB
README.md
5/27/2024 9:00 AM
MD File
6 KB
Type here to search
31°C
9:00 AM
5/27/2024

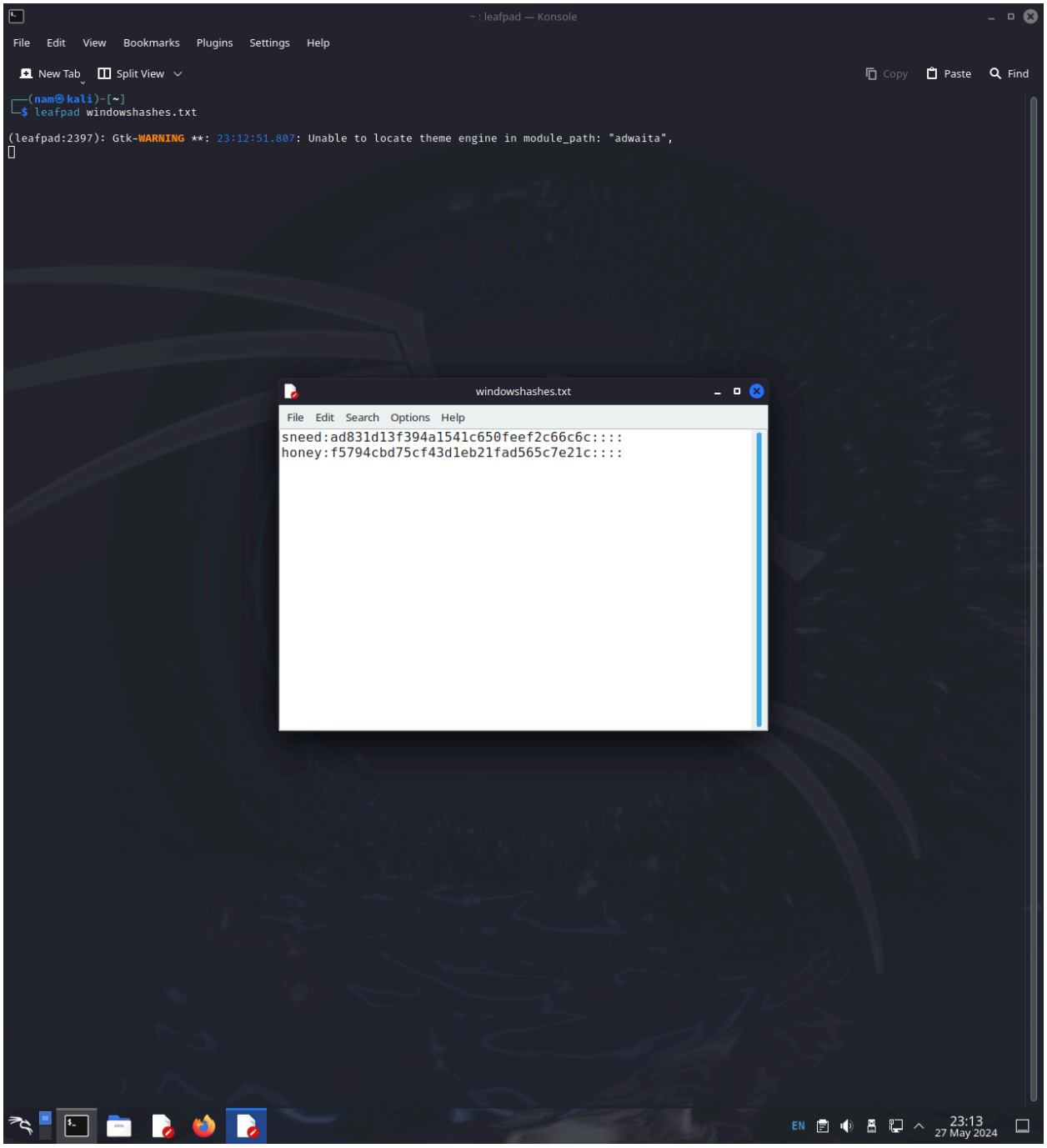

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
DefaultAcco...
A user account managed by the s...
defaultuser0
Guest
nam
WDAGUtility...
New User
User name: sneed
Full name: feed
Description: chuck
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
Actions
Users
More Actions
Type here to search
31°C
9:02 AM
5/27/2024

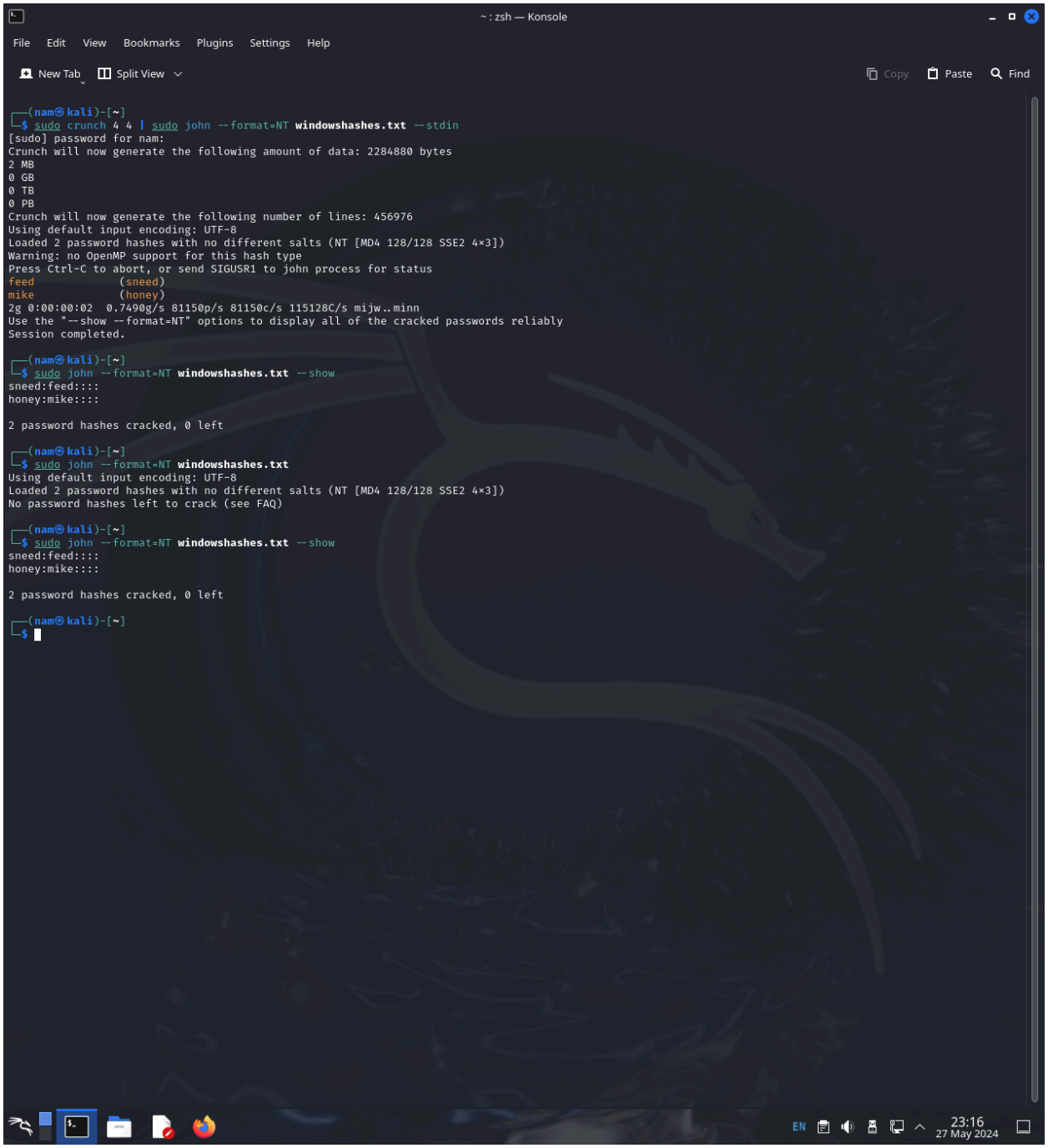

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
DefaultAcco...
A user account managed by the s...
defaultuser0
Guest
nam
sneed
WDAGUtility...
New User
User name: honey
Full name: mike
Description:
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
Actions
Users
More Actions
Type here to search
31°C
9:02 AM
5/27/2024


mimikatz 2.2.0 x64 (oe.eo)
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM
644 {0;000003e7} 1 D 23812 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0;00049570} 1 F 21023605 DESKTOP-BSUP848\nam S-1-5-21-3690152112-4110089468-4187489721-1001 (14g,24p) Primary
* Thread Token : {0;000003e7} 1 D 21587135 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)
mimikatz # log hashes.txt
Using 'hashes.txt' for logfile : OK
mimikatz # lsadump::sam sam.hiv system.hiv
Domain : DESKTOP-BSUP848
SysKey : 2b75dbf3ba9956b9d5620a0d061d974f
Local SID : S-1-5-21-3690152112-4110089468-4187489721
SAMKey : 3ad04a6e8472e8b665eb28ec2dd5fa29
RID : 000001f4 (500)
User : Administrator
RID : 000001f5 (501)
User : Guest
RID : 000001f7 (503)
User : DefaultAccount
RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 7406ecd87f378a49cba75ab739e83ebf
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 1c90b4f020d7c6b99d291d9a7f3e7493
* Primary:Kerberos-Newer-Keys *
Type here to search
31°C
9:06 AM
5/27/2024

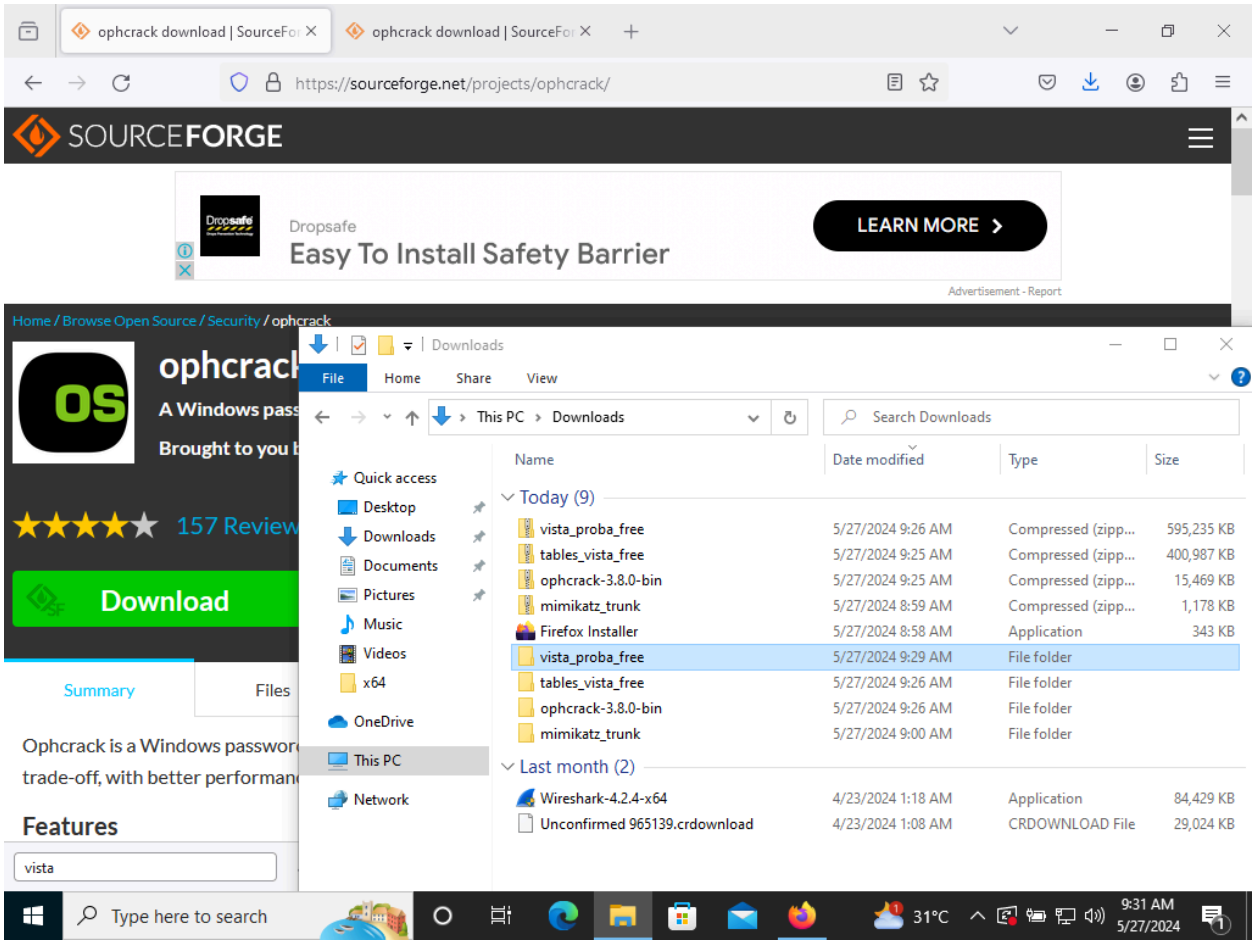

hashes - Notepad
File Edit Format View Help
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : DESKTOP-BSUP848nam
Credentials
des_cbc_md5 : 1679fb23f8a1688f
OldCredentials
des_cbc_md5 : 1679fb23f8a1688f
RID : 000003ea (1002)
User : sneed
Hash NTLM: ad831d13f394a1541c650feef2c66c6c
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 637a7e0efe5fbf551a55897e0821b5a4
* Primary:Kerberos-Newer-Keys *
Default Salt : DESKTOP-BSUP848sneed
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 61744b7ec160f2c79d374ed634d297f963f254264e7a16602c75fa95312610c3
aes128_hmac (4096) : dbb191dc3ae8a1dbd3d2ce73cff5a8d1
des_cbc_md5 (4096) : ce5438f2f7a85e73
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : DESKTOP-BSUP848sneed
Credentials
des_cbc_md5 : ce5438f2f7a85e73
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
Type here to search
31°C
9:07 AM
5/27/2024

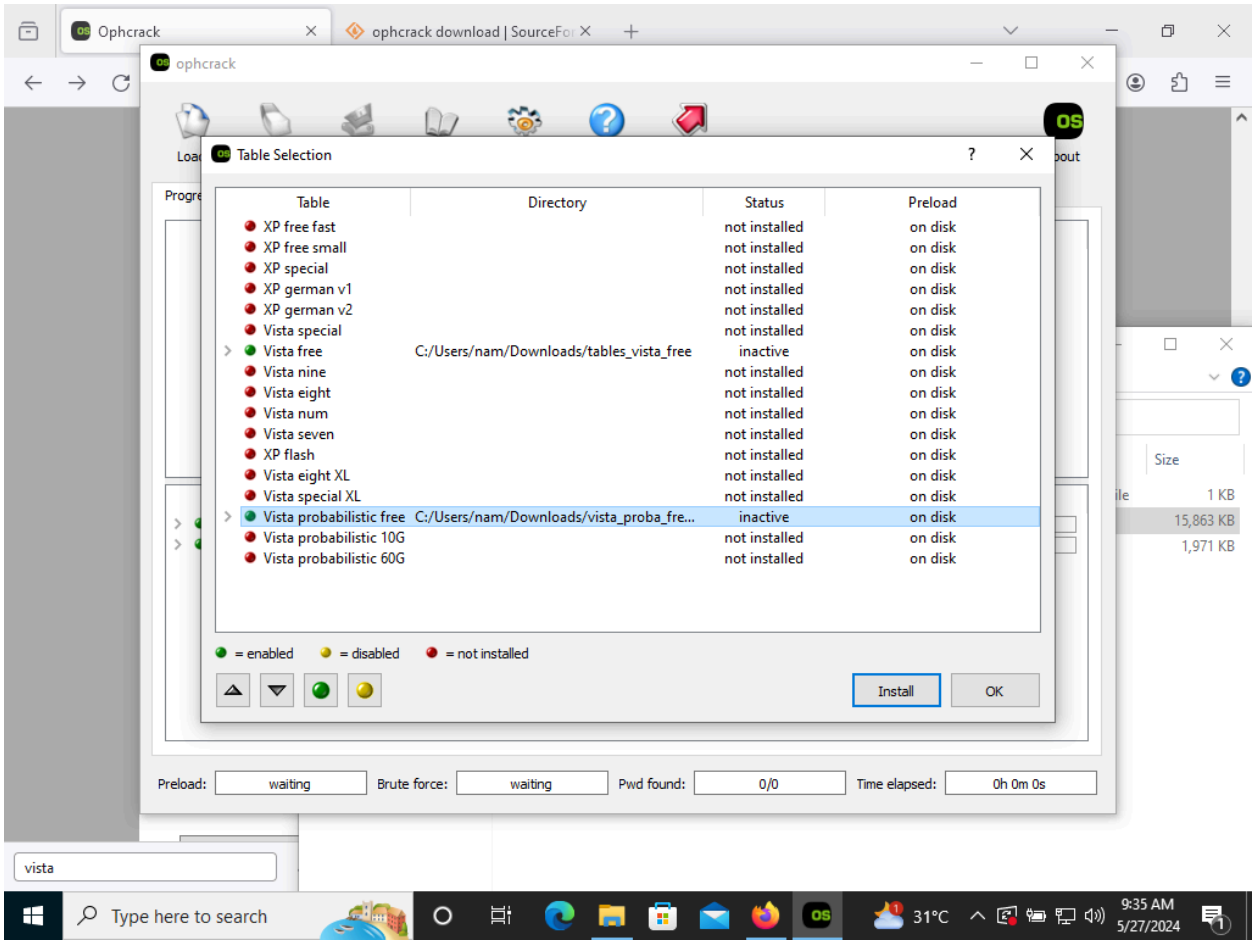

formattedhashes - Notepad
File Edit Format View Help
sneed:ad831d13f394a1541c650feef2c66c6c::::
honey:f5794cbd75cf43d1eb21fad565c7e21c::::
Ln 2, Col 43
100%
Windows (CRLF)
UTF-8
hashes - Notepad
File Edit Format View Help
User : sneed
Hash NTLM: ad831d13f394a1541c650feef2c66c6c
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 637a7e0efe5fbf551a55897e0821b5a4
* Primary:Kerberos-Newer-Keys *
Default Salt : DESKTOP-BSUP848sneed
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 61744b7ec160f2c79d374ed634d2
aes128_hmac (4096) : dbb191dc3ae8a1dbd3d2ce73cff5
des_cbc_md5 (4096) : ce5438f2f7a85e73
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : DESKTOP-BSUP848sneed
Credentials
des_cbc_md5 : ce5438f2f7a85e73
RID : 000003eb (1003)
User : honey
Hash NTLM: f5794cbd75cf43d1eb21fad565c7e21c
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 433fb3d3cff40a7be63d7ffa892cf626
* Primary:Kerberos-Newer-Keys *
Default Salt : DESKTOP-BSUP848honey
Default Iterations : 4096
Ln 133, Col 46
100%
Windows (CRLF)
UTF-8
Type here to search
31°C
9:09 AM
5/27/2024

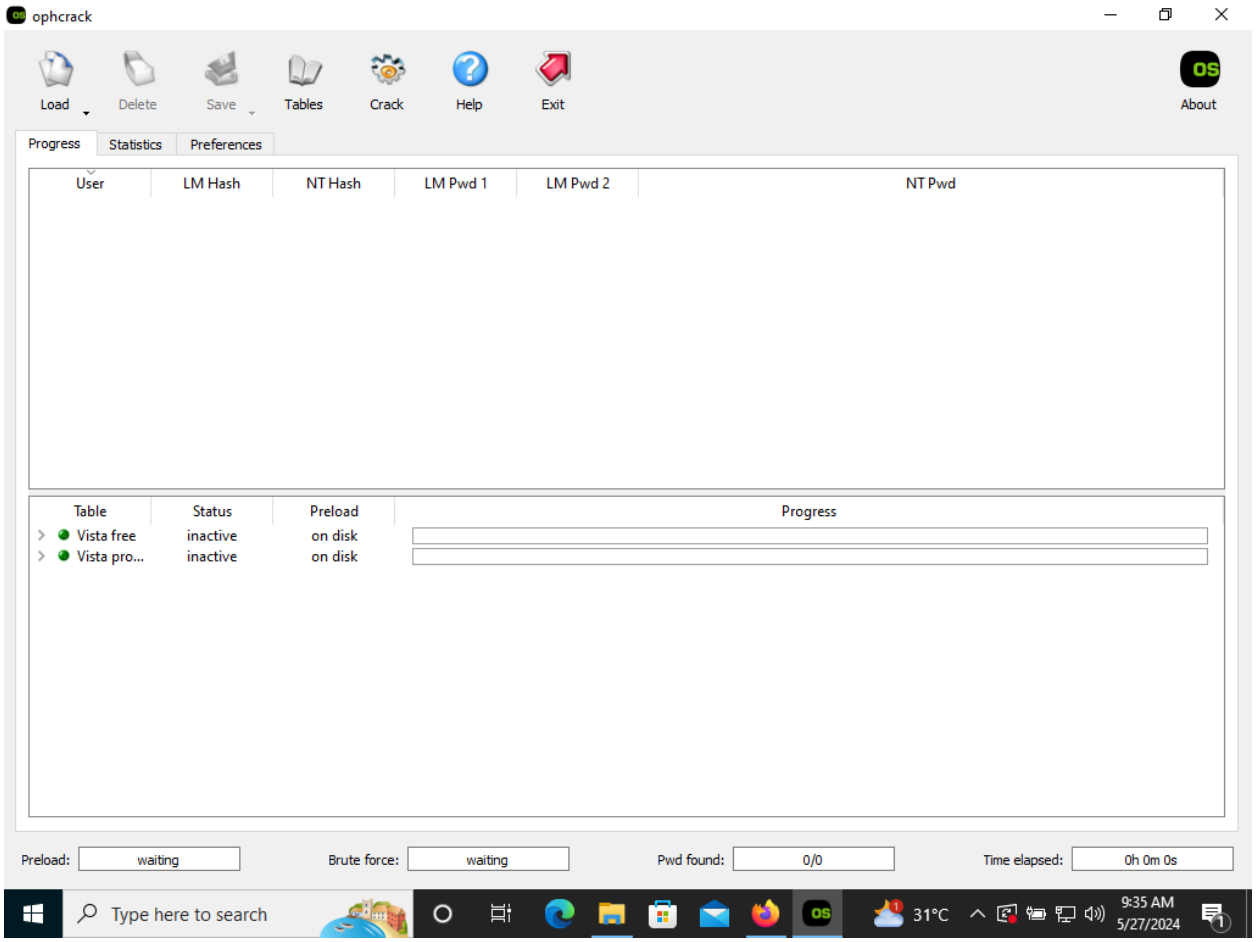

~ : leafpad — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab
Split View
Copy
Paste
Find
(nam㉿kali)-[~]
$ leafpad windowshashes.txt
(leafpad:2397): Gtk-WARNING **: 23:12:51.807: Unable to locate theme engine in module_path: "adwaita",
windowshashes.txt
File Edit Search Options Help
sneed:ad831d13f394a1541c650feef2c66c6c::::
honey:f5794cbd75cf43d1eb21fad565c7e21c::::
EN
23:13
27 May 2024

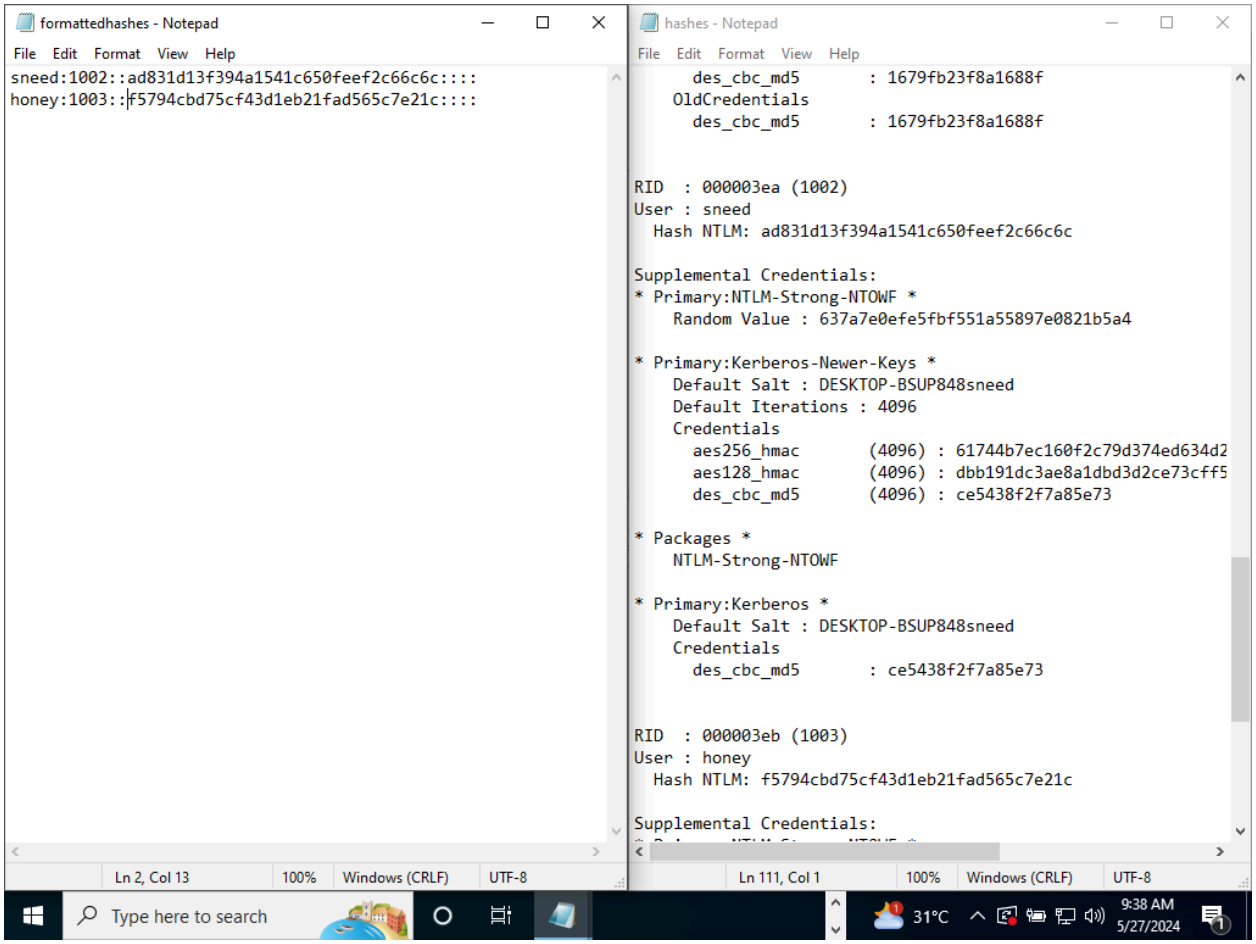

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
┌──(nam㉿kali)-[~]
└─$ sudo crunch 4 4 | sudo john --format=NT windowshashes.txt --stdin
[sudo] password for nam:
Crunch will now generate the following amount of data: 2284880 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 456976
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
feed (sneed)
mike (honey)
2g 0:00:00:02 0.7490g/s 81150p/s 81150c/s 115128C/s mijw..minn
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
┌──(nam㉿kali)-[~]
└─$ sudo john --format=NT windowshashes.txt --show
sneed:feed::::
honey:mike::::
2 password hashes cracked, 0 left
┌──(nam㉿kali)-[~]
└─$ sudo john --format=NT windowshashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 SSE2 4×3])
No password hashes left to crack (see FAQ)
┌──(nam㉿kali)-[~]
└─$ sudo john --format=NT windowshashes.txt --show
sneed:feed::::
honey:mike::::
2 password hashes cracked, 0 left
┌──(nam㉿kali)-[~]
└─$
EN
23:16
27 May 2024

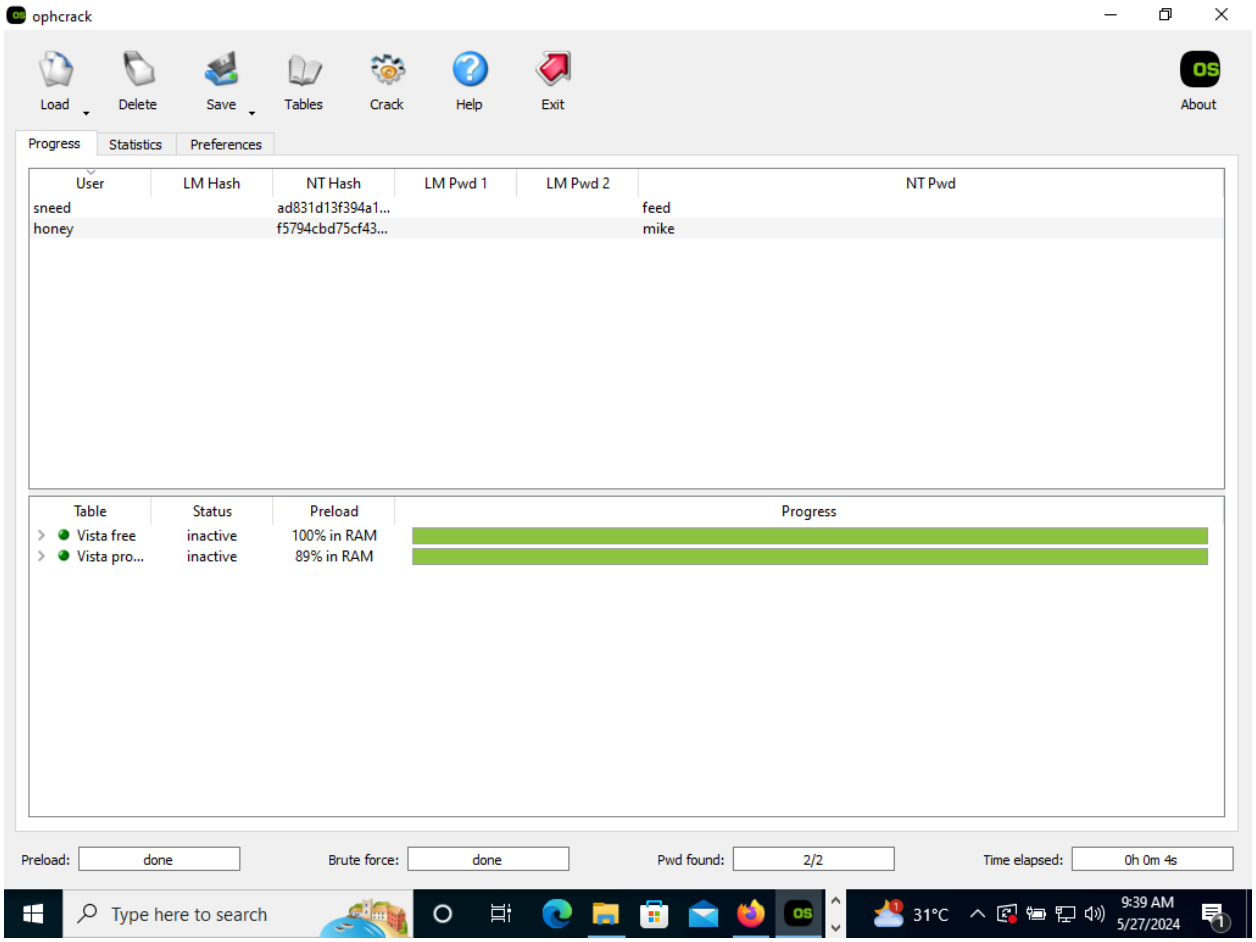
11.04

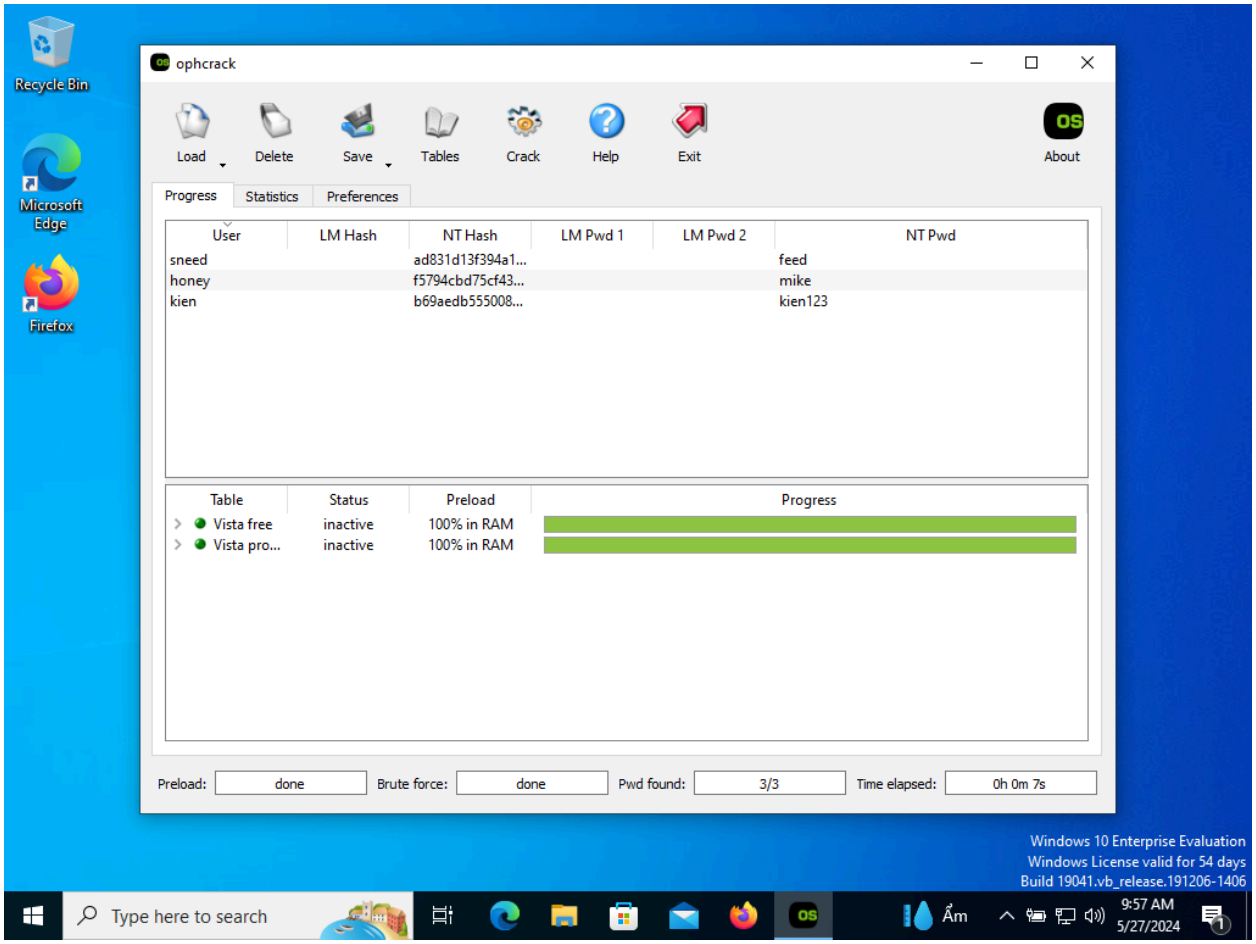

ophcrack download | SourceFo
ophcrack download | SourceFo
https://sourceforge.net/projects/ophcrack/
SOURCEFORGE
Dropsafe
Easy To Install Safety Barrier
LEARN MORE
Advertisement - Report
Home / Browse Open Source / Security / ophcrack
ophcrack
A Windows pass
Brought to you b
157 Review
Download
Summary
Files
Ophcrack is a Windows passwor
trade-off, with better performan
Features
vista
Downloads
File
Home
Share
View
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
x64
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (9)
vista_proba_free 5/27/2024 9:26 AM Compressed (zipp... 595,235 KB
tables_vista_free 5/27/2024 9:25 AM Compressed (zipp... 400,987 KB
ophcrack-3.8.0-bin 5/27/2024 9:25 AM Compressed (zipp... 15,469 KB
mimikatz_trunk 5/27/2024 8:59 AM Compressed (zipp... 1,178 KB
Firefox Installer 5/27/2024 8:58 AM Application 343 KB
vista_proba_free 5/27/2024 9:29 AM File folder
tables_vista_free 5/27/2024 9:26 AM File folder
ophcrack-3.8.0-bin 5/27/2024 9:26 AM File folder
mimikatz_trunk 5/27/2024 9:00 AM File folder
Last month (2)
Wireshark-4.2.4-x64 4/23/2024 1:18 AM Application 84,429 KB
Unconfirmed 965139.crdownload 4/23/2024 1:08 AM CRDOWNLOAD File 29,024 KB
Type here to search
31°C
9:31 AM
5/27/2024

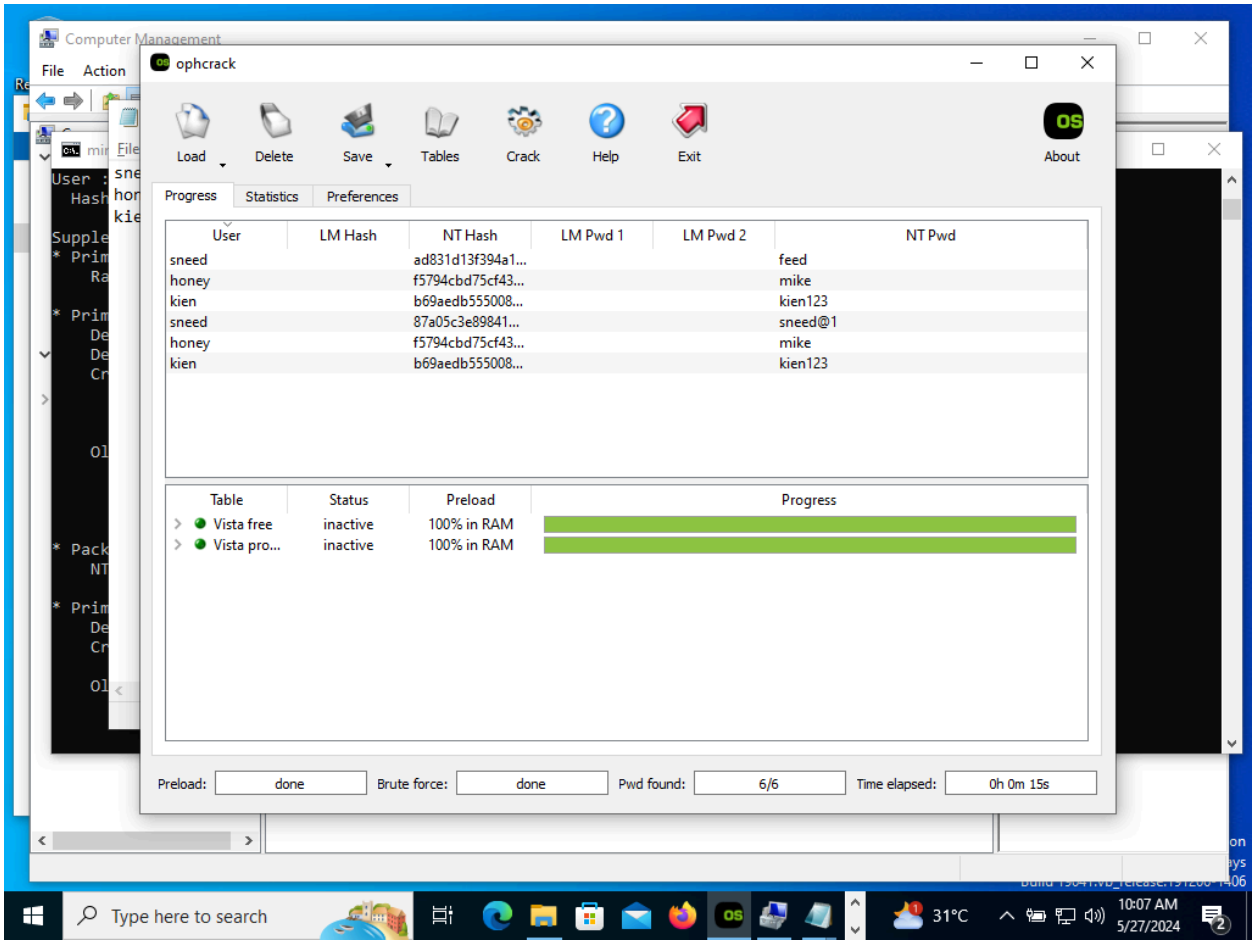

Ophcrack
ophcrack download | SourceFo
ophcrack
Table Selection
Table
Directory
Status
Preload
XP free fast
not installed
on disk
XP free small
not installed
on disk
XP special
not installed
on disk
XP german v1
not installed
on disk
XP german v2
not installed
on disk
Vista special
not installed
on disk
Vista free
C:/Users/nam/Downloads/tables_vista_free
inactive
on disk
Vista nine
not installed
on disk
Vista eight
not installed
on disk
Vista num
not installed
on disk
Vista seven
not installed
on disk
XP flash
not installed
on disk
Vista eight XL
not installed
on disk
Vista special XL
not installed
on disk
Vista probabilistic free
C:/Users/nam/Downloads/vista_proba_fre...
inactive
on disk
Vista probabilistic 10G
not installed
on disk
Vista probabilistic 60G
not installed
on disk
= enabled
= disabled
= not installed
Install
OK
Preload:
waiting
Brute force:
waiting
Pwd found:
0/0
Time elapsed:
0h 0m 0s
vista
Type here to search
31°C
9:35 AM
5/27/2024


ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Table
Status
Preload
Progress
Vista free
inactive
on disk
Vista pro...
inactive
on disk
Preload:
waiting
Brute force:
waiting
Pwd found:
0/0
Time elapsed:
0h 0m 0s
Type here to search
31°C
9:35 AM
5/27/2024


formattedhashes - Notepad
File Edit Format View Help
sneed:1002::ad831d13f394a1541c650feef2c66c6c::::
honey:1003::f5794cbd75cf43d1eb21fad565c7e21c::::
Ln 2, Col 13
100%
Windows (CRLF)
UTF-8
hashes - Notepad
File Edit Format View Help
des_cbc_md5 : 1679fb23f8a1688f
OldCredentials
des_cbc_md5 : 1679fb23f8a1688f
RID : 000003ea (1002)
User : sneed
Hash NTLM: ad831d13f394a1541c650feef2c66c6c
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 637a7e0efe5fbf551a55897e0821b5a4
* Primary:Kerberos-Newer-Keys *
Default Salt : DESKTOP-BSUP848sneed
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 61744b7ec160f2c79d374ed634d2
aes128_hmac (4096) : dbb191dc3ae8a1dbd3d2ce73cff5
des_cbc_md5 (4096) : ce5438f2f7a85e73
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : DESKTOP-BSUP848sneed
Credentials
des_cbc_md5 : ce5438f2f7a85e73
RID : 000003eb (1003)
User : honey
Hash NTLM: f5794cbd75cf43d1eb21fad565c7e21c
Supplemental Credentials:
Ln 111, Col 1
100%
Windows (CRLF)
UTF-8
Type here to search
31°C
9:38 AM
5/27/2024


ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
sneed
ad831d13f394a1...
feed
honey
f5794cbd75cf43...
mike
Table
Status
Preload
Progress
Vista free
inactive
100% in RAM
Vista pro...
inactive
89% in RAM
Preload:
done
Brute force:
done
Pwd found:
2/2
Time elapsed:
0h 0m 4s
Type here to search
31°C
9:39 AM
5/27/2024


Recycle Bin
Microsoft Edge
Firefox
ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
sneed
ad831d13f394a1...
feed
honey
f5794cbd75cf43...
mike
kien
b69aedb555008...
kien123
Table
Status
Preload
Progress
Vista free
inactive
100% in RAM
Vista pro...
inactive
100% in RAM
Preload:
done
Brute force:
done
Pwd found:
3/3
Time elapsed:
0h 0m 7s
Windows 10 Enterprise Evaluation
Windows License valid for 54 days
Build 19041.vb_release.191206-1406
Type here to search
9:57 AM
5/27/2024


Computer Management
File Action
ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User | LM Hash | NT Hash | LM Pwd 1 | LM Pwd 2 | NT Pwd
sneed | ad831d13f394a1... | feed
honey | f5794cbd75cf43... | mike
kien | b69aedb555008... | kien123
sneed | 87a05c3e89841... | sneed@1
honey | f5794cbd75cf43... | mike
kien | b69aedb555008... | kien123
Table | Status | Preload | Progress
Vista free | inactive | 100% in RAM
Vista pro... | inactive | 100% in RAM
Preload: done
Brute force: done
Pwd found: 6/6
Time elapsed: 0h 0m 15s
Type here to search
31°C
10:07 AM
5/27/2024