KPMG

IT Advisory

Windows passwords security

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

WHOAMI

Agenda

- The typical windows environment

- Local passwords
  - Secure storage mechanims: Syskey & SAM File
  - Password hashing & Cracking: LM & NTLM

- Into the domain
  - LSA secret & cached credentials

The typical Windows environment

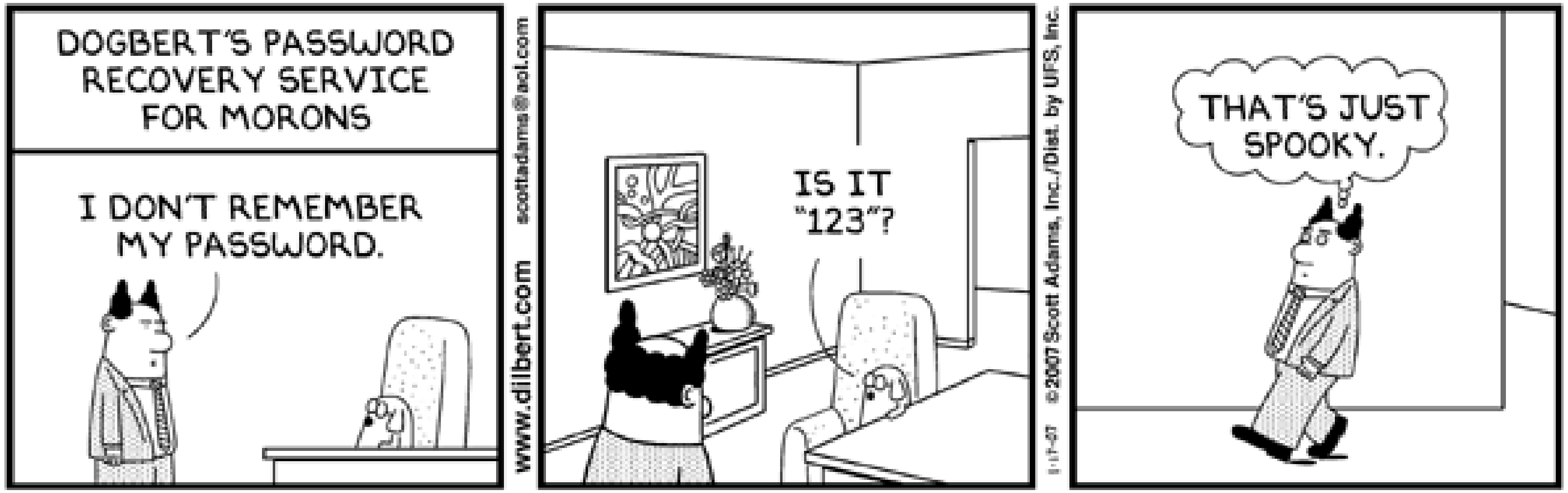
- Active directory
  - Centralized identification & authentication
    - Kerberos, NTLM and LM

- Local accounts (e.g. local admin)
- Processes running with domain service accounts
  - E.g. backup/virus agents

- Laptops
  - Requirements for offline authentication
    - Cached credentials

- **Conclusion:** Need secure storage in Windows

Remember: User is weakest link


DOGBERT'S PASSWORD RECOVERY SERVICE FOR MORONS
I DON'T REMEMBER MY PASSWORD.
scottadams@aol.com
www.dilbert.com
IS IT "123"?
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
THAT'S JUST SPOOKY.

© Scott Adams, Inc./Dist. by UFS, Inc.

Secure storage

- Syskey: Boot key used as master key for secure contents
  - Implementation:
    - Syskey on floppy @boot
    - Syskey derived from passphrase @boot
    - Syskey on the system: Obfuscation

Not feasible for
remote administration

  - Stored in register SYSTEM\CurrentControlSet\Control\Lsa\{JD,Skew1,GBG,Data}
  - Cannot be read with normal tools (regedit)
  - Stored in c:\windows\system32\config\system
  - Exclusively locked by kernel/System user

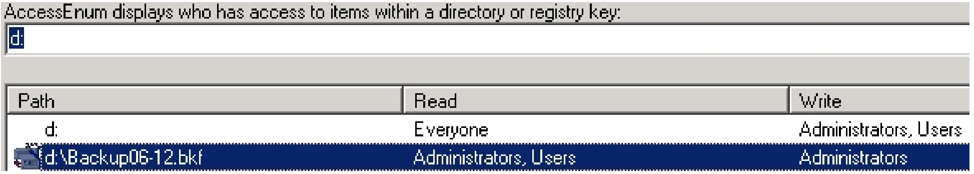
- Security Accounts Manager (SAM) file
  - Encrypted with Syskey (as of Win2000)
  - Contains hashes of password (more later)
  - Same security/storage mechanism as Syskey (C:\windows\system32\config\SAM)

Attacking Syskey & SAM file

- Get SYSTEM/Kernel privilege
  - Requires administrative access (Local exploit)

- Physical access:
  - Boot other OS
  - Copy c:\windows\system32\config\system and c:\windows\system32\config\SAM
  - Crack passwords (more later)
  - Adjust SAM file (create new local admin)

- Or do it the easy way:
  - Use backups ☺
    - C:\windows\repair or other back-ups



AccessEnum displays who has access to items within a directory or registry key:

d:

Path	Read	Write
d:	Everyone	Administrators, Users
d:\Backup06-12.bkf	Administrators, Users	Administrators

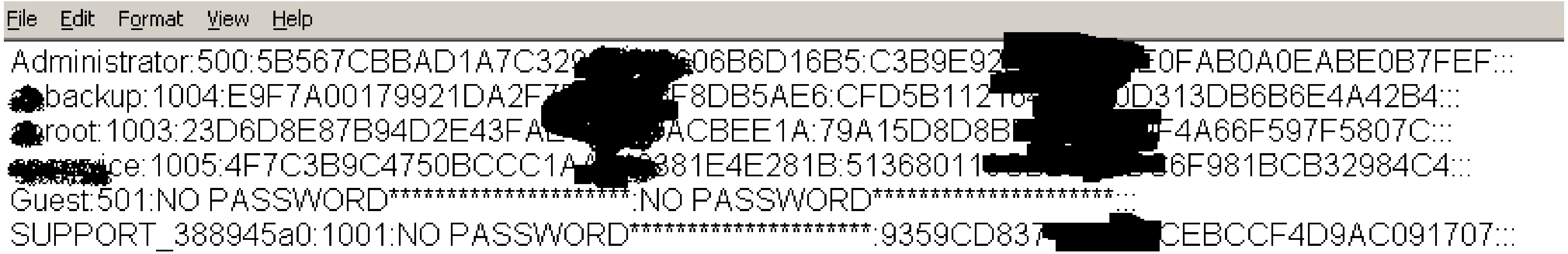
- Tools:

TEXT REMOVED, SEE REFERENCES

PWdump: How does it work

- TEXT REMOVED, PLEASE REFER TO http://us1.samba.org/samba/ftp/pwdump/pwdump.c

Results so far: A SAM file



```
Administrator:500:5B567CBBAD1A7C32[redacted]06B6D16B5:C3B9E92[redacted]E0FAB0A0EABE0B7FEF:::
[redacted]backup:1004:E9F7A00179921DA2F[redacted]F8DB5AE6:CFD5B112[redacted]D313DB6B6E4A42B4:::
[redacted]root:1003:23D6D8E87B94D2E43FA[redacted]ACBEE1A:79A15D8D8B[redacted]F4A66F597F5807C:::
[redacted]ce:1005:4F7C3B9C4750BCCC1A[redacted]381E4E281B:51368011[redacted]6F981BCB32984C4:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
SUPPORT_388945a0:1001:NO PASSWORD*********************:9359CD837[redacted]CEBCCF4D9AC091707:::
```

- Format:

  Username: ID: LM hash: NTLM hash:::

Lan Manager Hashes

- History
  - Microsoft Lan Manager (OS) introduced in 198?
  - Main MS server OS until NT 3.1 (1993)

- All Windows versions before Vista/2008 server: Enabled by default

  In Vista/2008 server it can be enabled

- Current use:
  - Legacy communication (Mainframe)
  - CIFS

Lan manager hashing

- ANSI password is tranfered to uppercase only
- Padding with null until 14 bytes
- Split in two 7-byte arrays
- Calculate partiy and add to array (result: 64bits)
- DES-encrypt the string “KGS!@#$%” using the array as key (2x)
- Concatenate 2 cipertexts

ANSI not unicode

Uppercase,
reduce entropy

LM fails with length>14

No freshness/salting

Determine if pwlength<7

Attacking LM hashes

- Ideal: 95^14 different passwords, (approx 2^92)

- Uppercase: 67^14

- Split in two 7 char: 67^7 (approx 2^43)

- No salting: Memory-Time tradeoff - Rainbow tabless
  - LM hashes are cracked within a couple of minutes (rcrack)
  - CPU cracking in hours (john)

- By inspecting the second part of the LM-value, you can determine if the password had more than 7 characters

NTLM background

- New Technology Lan Manager (NTLM)
  - Both hash storage and communication protocol

- NTLM-communication:
  - NTLMv1
    - Introduced with Windows NT 3.1 (1993)
    - Overcome problems with LM (e.g. unicode, hashing)
    - Backwards compatible with LM
  - NTLMv2
    - Introduced with NT4 SP4, (1998)
    - Cryptographic improvements over NTLMv1

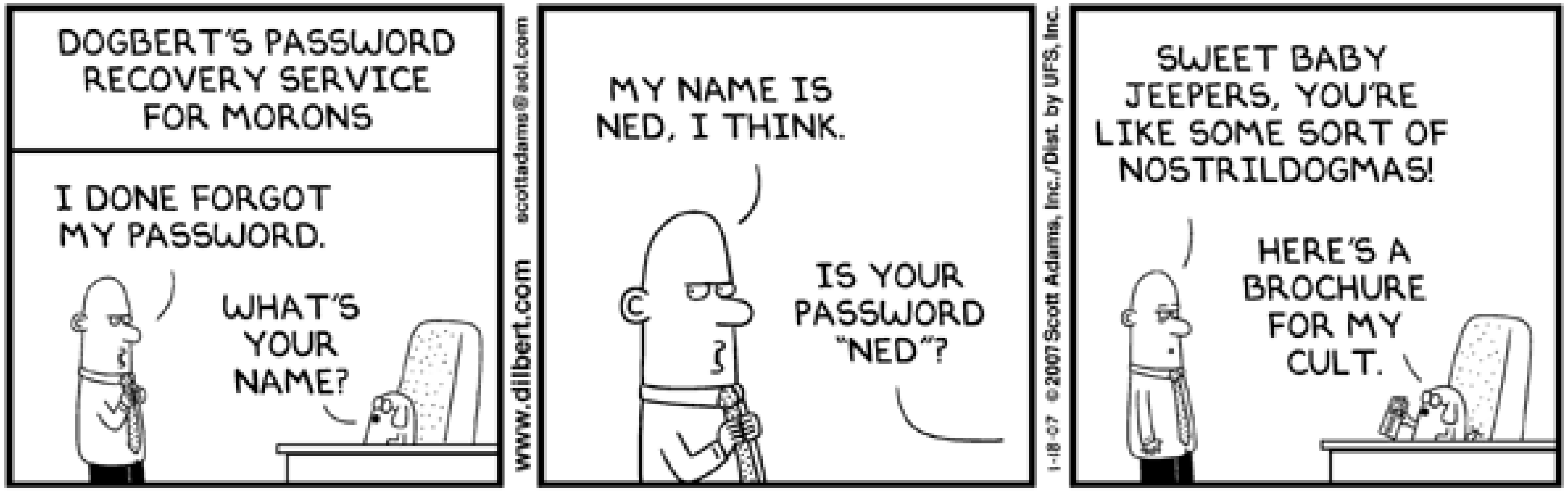
NTLM hash algorithm

- Simple:
  - MD4(password)

  - No salting, thus memory/space tradeoff
  - 128 bit

  - Tools: John (bruteforce), Rcrack(rainbow tables), multiforcer (GPU cracking bruteforce)

Remember: Users are weakest link


DOGBERT'S PASSWORD RECOVERY SERVICE FOR MORONS
I DONE FORGOT MY PASSWORD.
WHAT'S YOUR NAME?
www.dilbert.com scottadams@aol.com
MY NAME IS NED, I THINK.
IS YOUR PASSWORD "NED"?
1-8-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.
SWEET BABY JEEPERS, YOU'RE LIKE SOME SORT OF NOSTRILDOGMAS!
HERE'S A BROCHURE FOR MY CULT.

© Scott Adams, Inc./Dist. by UFS, Inc.

Summary: Putting it all together

LOADING

IRONGeek
Lifting dumbbells in the gym,
supporting them at work.

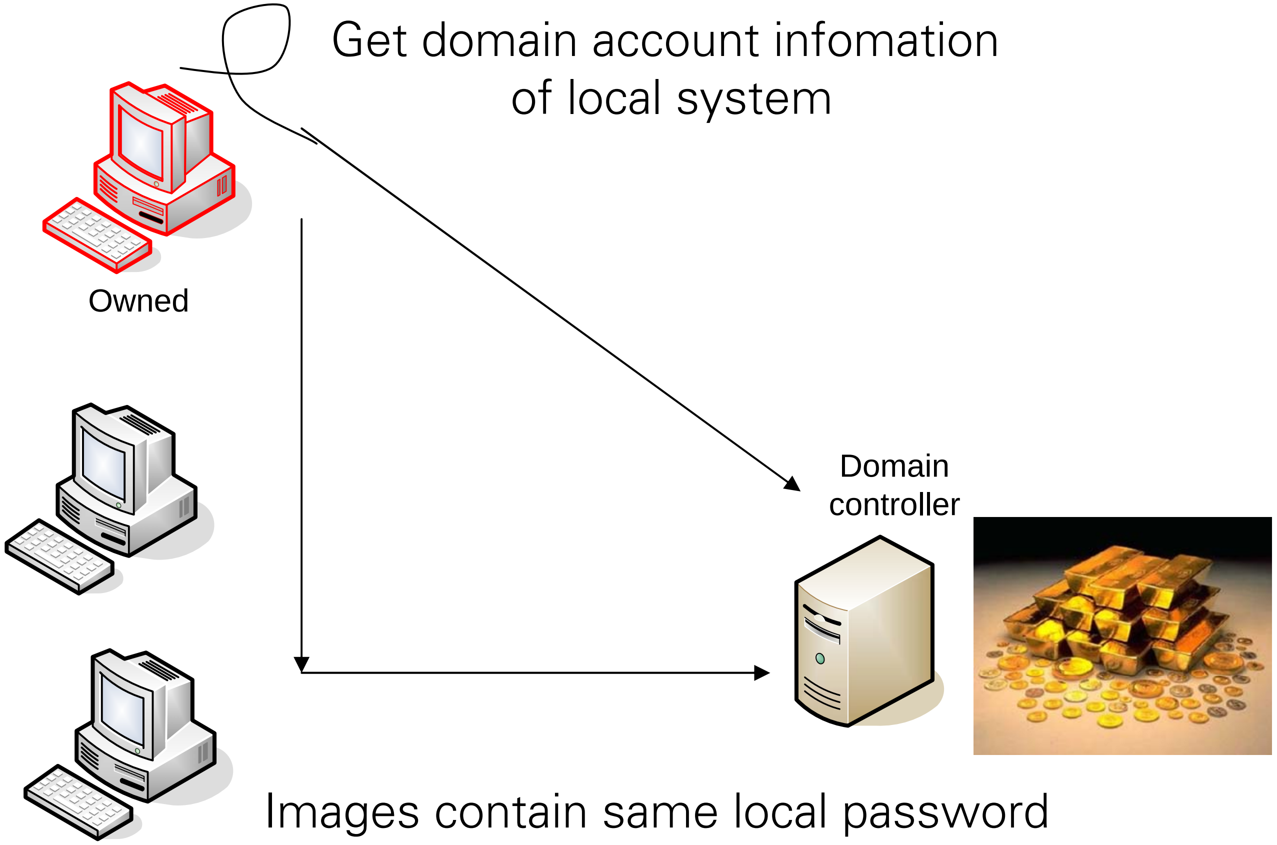
Example SAM file

- testuser1:"":0F20048EFC645D0A179B4D5D6690BDF3:1120ACB74670C7DD46F1D3F5038A5CE8:::
- remote:"":E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C:::
- joeuser:"":E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C:::
- averageguy:"":299CCF964D9A359BAAD3B435B51404EE:A5C07214487C87B584E8877DE72DCA0B:::
- harderpass:"":B75838F7A57EE67993E28745B8BF4BA6:EC50F8A8149C93EF45AECB8AF96658E6:::
- demouser:"":261A6631FE44BA4993E28745B8BF4BA6:371D5760453C1B000BCC016F8E23A83C:::
- randy:"":98B5AFEB67293D6AAAD3B435B51404EE:A9F34664151F6360757B31644F37E025:::
- Asmith:"":E165F0192EF85EBBAAD3B435B51404EE:E4EBE0E7EF708DC9FD240135D3D43D89:::
- Bsmith:"":136A8418CF76C4F7AAD3B435B51404EE:3431E75AD08DCA56EB53AEAAB9926589:::
- csmith:"":BB26C063532826AA531C3383FDDBFF2A:A2746ED4129985C0251D2B968C4889FE:::

- What do you see?

- Online cracking: http://plain-text.info/

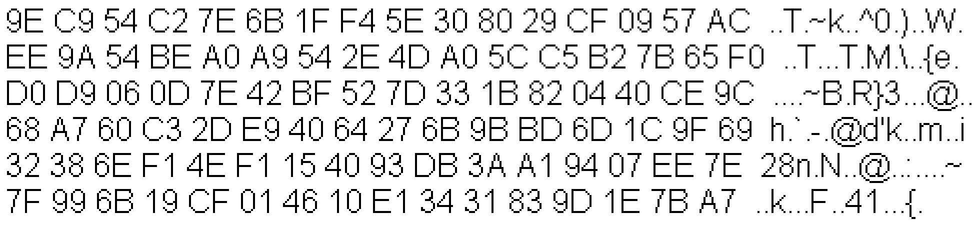
Getting into the domain



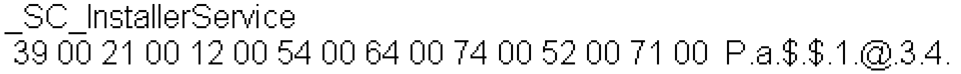
Images contain same local password
Keylogger on administrator station

LSA secrets & Cached credentials

- LSA secrets:
  - encrypted with SYSKEY
  - Contains up to 10 cached credentials
  - May contain passwords for service accounts



```
9E C9 54 C2 7E 6B 1F F4 5E 30 80 29 CF 09 57 AC  ..T.~k..^0.)..W.
EE 9A 54 BE A0 A9 54 2E 4D A0 5C C5 B2 7B 65 F0  ..T...T.M.\..{e.
D0 D9 06 0D 7E 42 BF 52 7D 33 1B 82 04 40 CE 9C  ....~B.R}3...@..
68 A7 60 C3 2D E9 40 64 27 6B 9B BD 6D 1C 9F 69  h.`.-.@d'k..m..i
32 38 6E F1 4E F1 15 40 93 DB 3A A1 94 07 EE 7E  28n.N..@..:....~
7F 99 6B 19 CF 01 46 10 E1 34 31 83 9D 1E 7B A7  ..k...F..41...{.
```



```
_SC_InstallerService
 39 00 21 00 12 00 54 00 64 00 74 00 52 00 71 00  P.a.$.$.1.@.3.4.
```

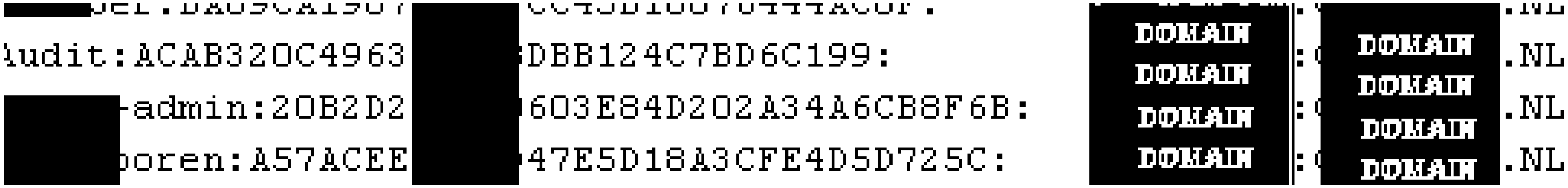
Password of account "_SC_InstallerService"

  - Tools: Cain, PwdumpX, LSAdump2

Cached credentials

- In LSA secrets cached credentials are stored (obfuscated)
- Maximum 10 accounts

- Tools: Pwdumpx, cain
- Format:
  UserName:95C0D475F5E0C888DD3E0F4D56CA3C75:ActiveDirectoryDomain:Domain



```
udit:ACAB320C4963[redacted]DBB124C7BD6C199:DOMAIN:DOMAIN.NL
[redacted]-admin:20B2D2[redacted]603E84D202A34A6CB8F6B:DOMAIN:DOMAIN.NL
[redacted]oren:A57ACEE[redacted]47E5D18A3CFE4D5D725C:DOMAIN:DOMAIN.NL
```

- Hash: MSCACHE = MD4(MD4(password) || lowercase(username))

- Salted with username, thus no rainbow tables
  - There is one for the “Administrator” account

- Tools: Cain, John with mscach patch, rcrack

Other interesting password stores

- IE passwords
- Messenger
- Outlook express
  - Use PSTGdump

- Firefox password store

- Or just search (outlook) mailbox

Fixing it:

- Disable LM hashing

- Don’t use passwords? Use smartcards/tokens…
  - Enable password complexity

- Minimize local accounts
- No password reuse between systems (images)

- Harden service accounts
- Minimize cached credentials
- Rename built in accounts

- Logging & monitoring

Questions?

References

- http://www.irongeek.com
- http://reedarvin.thearvins.com/tools/
- http://www.oxid.it/
- http://swamp.foofus.net/
- http://us1.samba.org/samba/ftp/pwdump/pwdump.c
- http://en.wikipedia.org/wiki/NTLM
- www.Dilbert.com

NTLM protocols

- NTLMv1
- Challenge-response
  - Server -> Client: Challenge
  - Cient->Server: split MD4(pass) in 3 chunks,
send DES(challenge, key[1])+
DES(challenge,key[2])+
DES(challenge,key[3])

Pieter Ceelen
KPMG Advisory N.V.
Phone 020 656 4062
ceelen.pieter@kpmg.nl
www.kpmg.nl