# AM PC 시스템 구축 보고서

| | |
|---|---|
| RED 담당자 | 동석 신 |
| 진행 상태 | 완료 |
| 마감일 | @2023년 8월 24일 |
| 최종 편집 일시 | @2023년 8월 31일 오후 11:11 |
| 최종 편집자 | 예린 주 |
| 프로젝트 | 프로젝트 환경 구축 |

ESXi에 아래 사항 진행

- OS 설치
- 애플리케이션 설치
- 윈도우 환경 설정(취약점 부여)
- 내부 네트워크 통신 확인

## 개요

제휴 담당자는 최초 감염 대상으로, 문서형 악성코드를 다운 받고 실행하여 내부 네트워크로 확산하기 위한 거점 역할을 수행하게 된다.

### 필요한 애플리케이션

- MS Office 16 (word)
- ms-msdt (기본 내장)
- 메일 관련 소프트웨어
- Chrome / Edge

### 윈도우 환경 설정

- SMB 관련 허용
- 공유 네트워크 / 폴더 허용

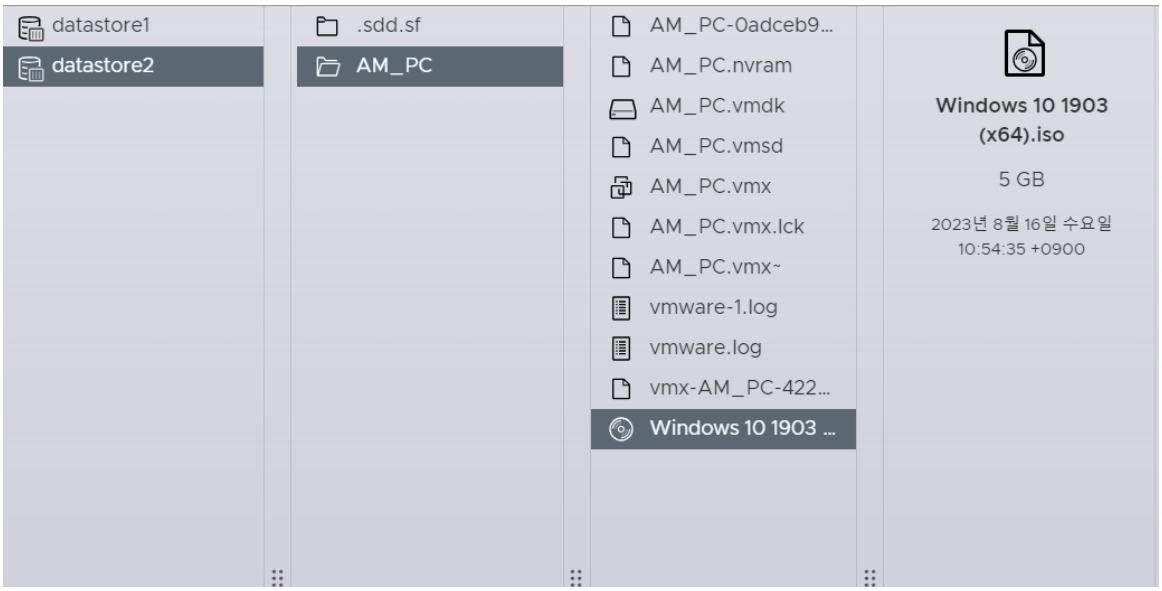
# 설정

아래 항목들에 대한 세팅을 진행한다

| 분류 | 항목 | 설명 |
|---|---|---|
| OS | Windows | OS 버전 및 최초 설정 |
| Application | MS OFFICE 16 | 문서 열람을 위한 MS 설치 |
| Application | Outlook | 메일 열람을 위한 메일 뷰어 설치 |
| | | |

제안서

## ▼ 윈도우 설치




ESXi AM_PC datastore

**OS : Windows 10 x64 1903 pro**

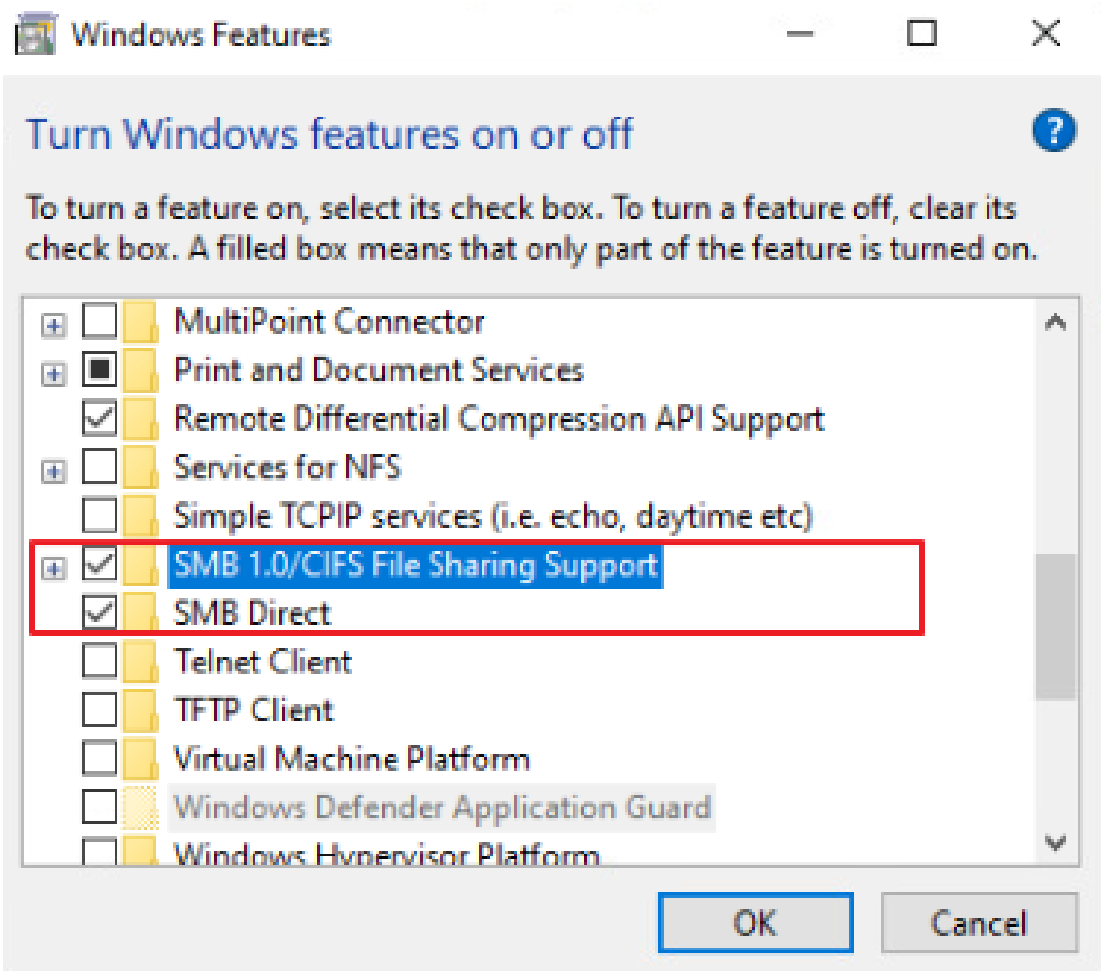

OS Version

최초 설치 후 SMB / defender / Windows update 설정을 진행한다.

1. **SMB**

   PM PC로 확산을 위해서 설정해야한다.

   **설정 켜기**




Windows Features / turn on SMB options

→ Control Panel\Programs\Programs and Features

**설정 확인**

```
C:\Users\DELL>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.


C:\Users\DELL>net user

User accounts for \\DESKTOP-F863PP3

-------------------------------------------------------------------------------
Administrator            DefaultAccount          defaultuser0
DELL                     Guest                   WDAGUtilityAccount
The command completed successfully.


C:\Users\DELL>
```

check SMB options using command line

2. **Defender**

   원활한 공격 테스트를 진행하기 위해서 실시간 보호 기능을 전부 내려둔다


Windows Security settings

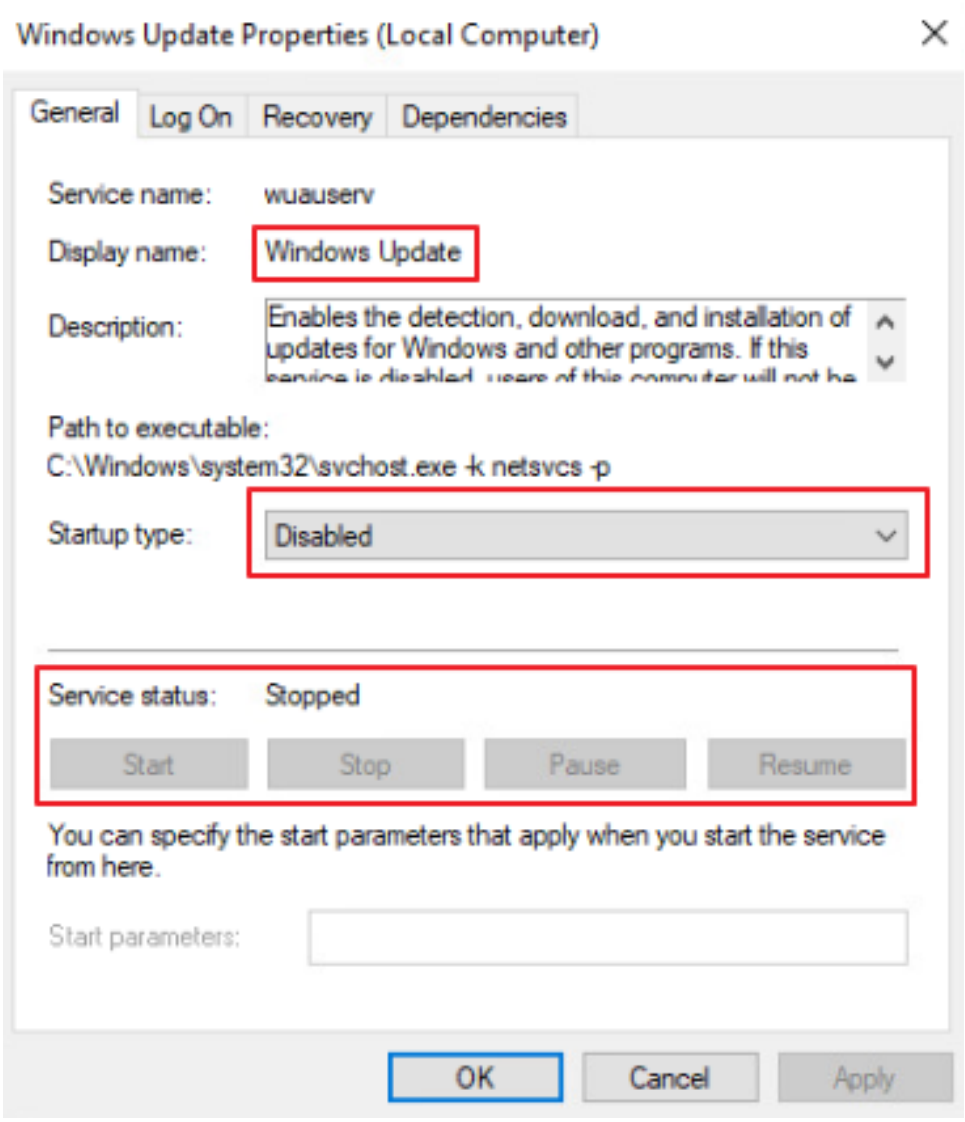
→ Windows Security\Virus & threat protection settings

아래 4개 항목 모두 꺼둔다.

- Real-time protection
- Cloud-delivered protection
- Automatic sample submission
- Tamper Protection

3. **Windows update**

   테스트 도중 윈도우 시스템 업데이트로 인해서 취약점 패치가 이루어지지 않도록 업데이트 관련 서비스를 꺼두어야 한다.




Services Properties

Services\Windows Update

## ▼ MS Office 16 설치

### 제한된 실행 해제하기


## ▼ Outlook

당장 테스트엔 사용하지 않지만, 추후에 사용하기 위해서 위 MS Office 16 설치 과정에서 함께 설치 진행

테스트용 구글 계정 새로 만들어서 진행