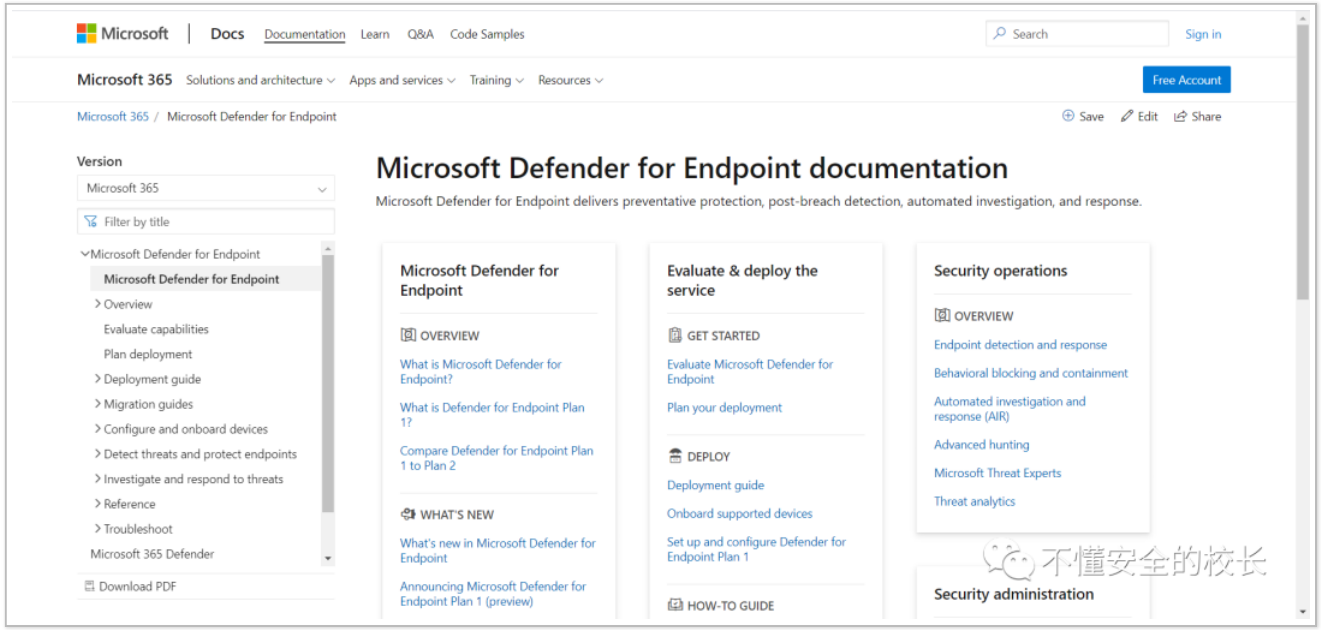
Bypass_AV – Windows Defender

0x01 官方文档

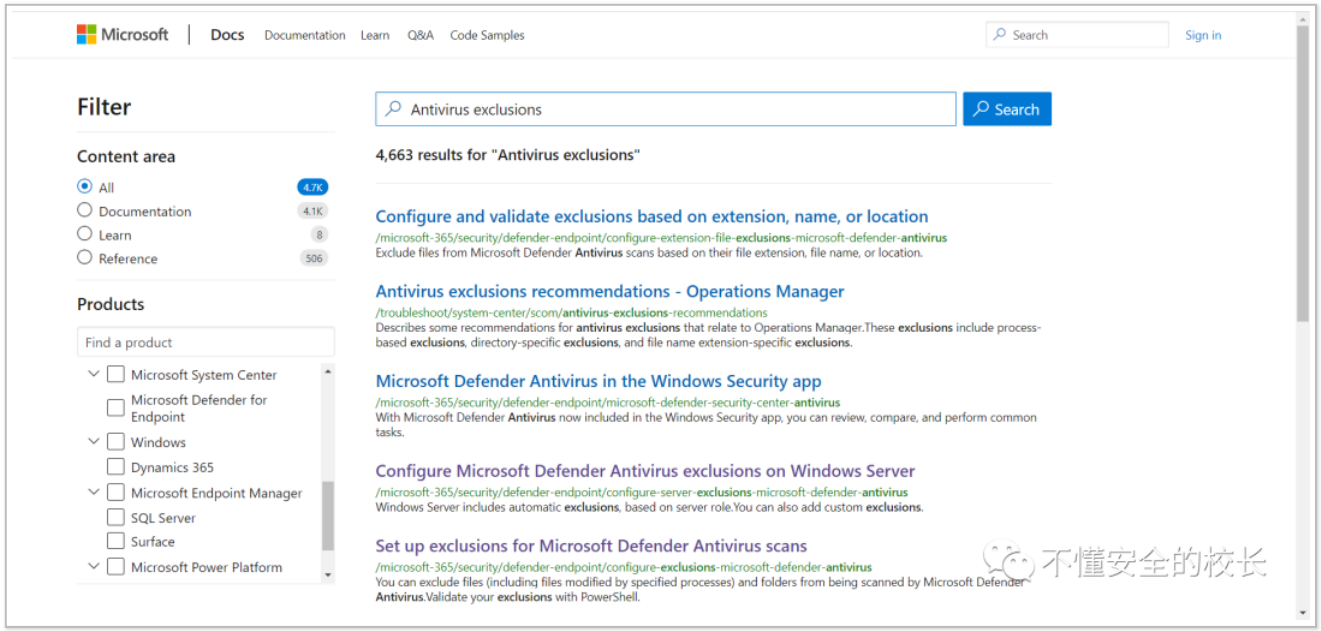
参考: `https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide`



我们可以从官方文档里面找到一些关于 Def 的资料，以及它扫描的时候排除什么，关注什么！通过它的疏忽我们来绕过 Windows Defender!

0x02 开始查找

搜索关键词: `Antivirus exclusions`



我找到了其中一个文档

参考文档: `https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-exclusions-microsoft-defender-antivirus?view=o365-worldwide`

概括

本文概述了 `Windows Server 2016` 或 `更高版本上Microsoft Defender` 防病毒的排除项。

由于 `Microsoft Defender` 防病毒软件内置于 `Windows Server 2016 及更高版本中` ，因此会自动排除操作系统文件和服务器角色。但是，您可以定义自定义排除项。如有必要，您还可以选择退出自动排除。

0x03 默认排除项

Web 服务器排除项本节列出了安装 `Web 服务器角色` 自动提供的**文件夹排除项**和**进程排除项**

文件夹排除

- `%SystemRoot%\IIS Temporary Compressed Files`
- `%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files`
- `%SystemDrive%\inetpub\temp\ASP Compiled Templates`
- `%systemDrive%\inetpub\logs`
- `%systemDrive%\inetpub\wwwroot`

进程排除

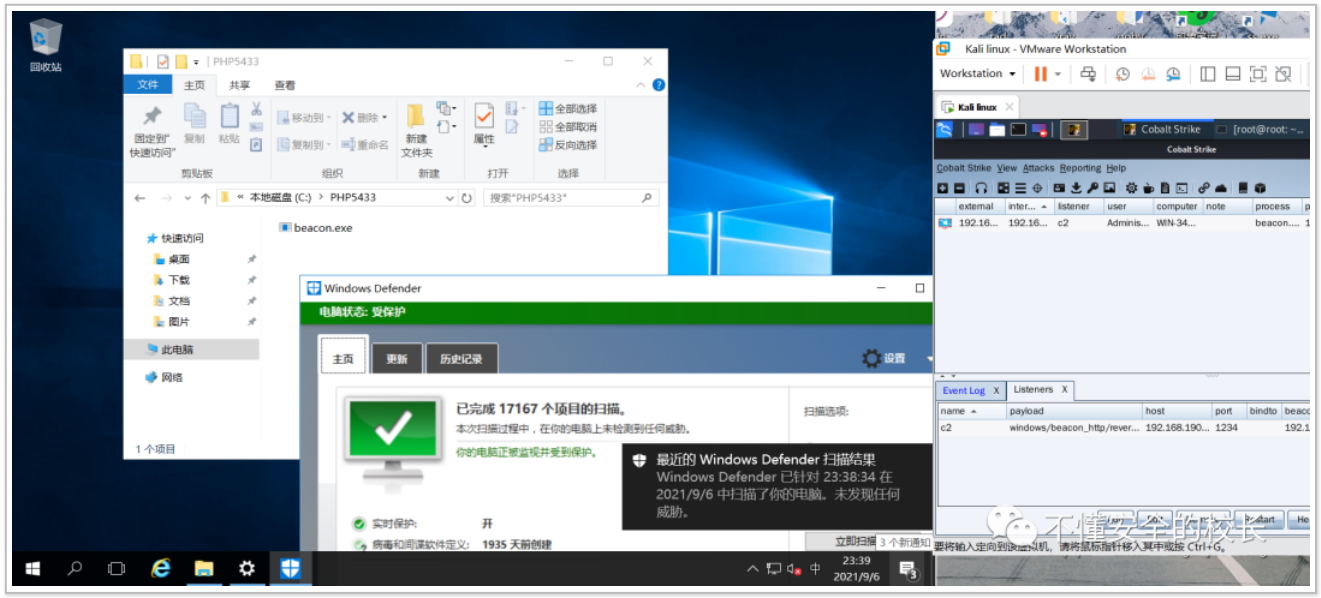
- `%SystemRoot%\system32\inetsrv\w3wp.exe`
- `%SystemRoot%\SysWOW64\inetsrv\w3wp.exe`
- `%SystemDrive%\PHP5433\php-cgi.exe`

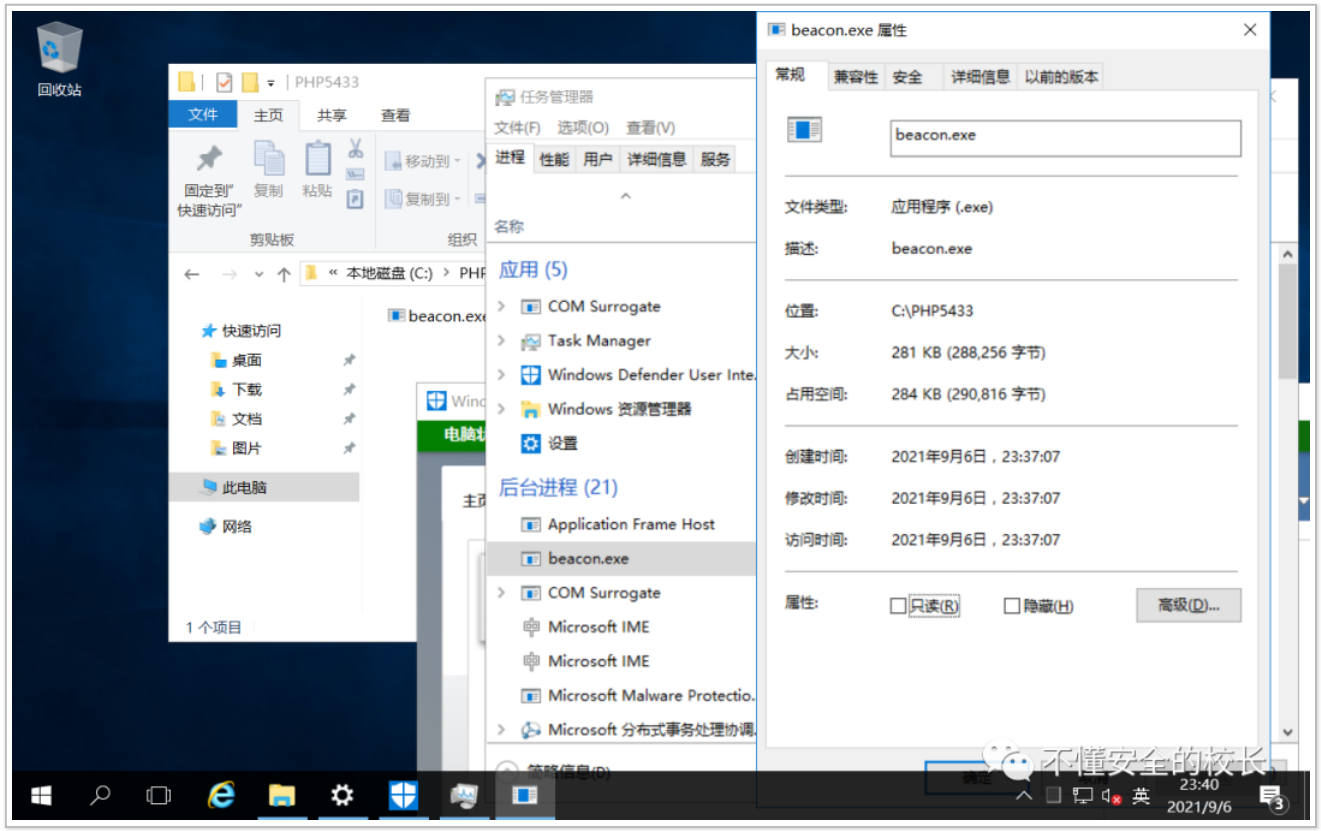
在检测过程中会忽略这些排除项，于是我们就能开始 Bypass_AV 了。这些文件路径在不冲突的情况下，都能够 Bypass Windows Defender!

以 `%SystemDrive%\PHP5433\php-cgi.exe` 为例子，我们来进行 Bypass 以 Windows Server 2016 为环境

环境下载链接: `https://msdn.itellyou.cn/`

在 `C:\` 目录下创建 `\PHP5433\`，使用 CS 生成. exe 文件放置在该目录下运行，看看 WIndows Defender 是什么反应。





成功运行，并且使用 Windows Defender 扫描不出来。但是在 Shell 下能否运行需要师傅们自行去测试！