赛博昆仑
CYBER KUNLUN

Windows Server NPS RCE 漏洞

漏洞情报速报

——攻防驱动数据安全

8 月 20 日

北京赛博昆仑科技有限公司

2023 年 8 月 19 日，赛博昆仑洞见产品捕获到利用 windows server NPS 服务漏洞进行远程代码执行攻击事件，攻击者可以利用该漏洞执行任意代码，最终实现获取域控的控制权。

该漏洞在 Windows Server 启用 Network Policy and Access Service(NPS)特性并配置 IAS Extension DCOM server 时会存在远程代码执行漏洞。

该漏洞存在于 IAS 的扩展服务中，属于 NPS 的范围，在启用 NPS 特性后即存在，配置远程的 IAS 扩展服务可用于允许远程用户调用 Server 端扩展 API 进行身份验证等操作。

该漏洞源自 iassam.dll，该漏洞为逻辑漏洞，根本原因是当 client 调用 ias extension host 接口请求扩展 dll API 时，传入路径为可控路径，但检查路径不严格，导致可以使用 remote unc 路径加载远程任意 dll，最终导致远程代码执行。

1. 漏洞详情

漏洞名称：windows server NPS 服务远程代码执行漏洞

威胁程度：

该漏洞是主要针对域控服务器进行攻击的，漏洞针对的 NPS 服务一般只有域控集权等认证服务器才会主动配置，只要进行了相关配置就可以利用该漏洞进行 RCE，该漏洞的最终目标是控制域控服务器，故该漏洞针对与域控服务器的威胁极大建议尽早排查和处置。

处置建议：

1、 查看 windows server 运行版本，确认是否在受影响版本范围内；

2、 临时禁用受影响版本 windwos server 上的 Network Policy and Access Service(NPS)服务；

3、 目前赛博昆仑洞见产品已经支持检测和修复该漏洞，建议服务器部署赛博昆仑洞见漏洞防御产品，确保对该漏洞后续的攻击利用行为的持续检测与响应。

漏洞类型： 0Day

厂商： 微软

漏洞官网链接： https://www.microsoft.com/zh-cn/

影响范围： Windows Server 2016/2019/2022 并开启 NPS 服务且配置 IAS 的域控环境

漏洞所在功能模块： NPS 的 IAS 扩展服务

漏洞攻击效果： 远程代码执行

漏洞关联产品介绍：

https://learn.microsoft.com/zh-cn/windows-server/networking/technologies/nps/nps-top

2. 漏洞原理

漏洞位于 iassam.dll，该漏洞为稳定触发的逻辑漏洞，具体漏洞代码如下：

```
```
__int64 __fastcall RadiusExtensionPoint::Load(
        RadiusExtensionPoint *this,
        enum _RADIUS_EXTENSION_POINT a2,
        const unsigned __int16 *uncpath)
{
[…]
if (!IsNT4Only(uncpath)) // ===> 检查 uncpath，但没检查 remote path 的情况
        {
          v5 = RadiusExtension::Load(*((RadiusExtension **)this + 2),
uncpath); // ===> 将可控 uncpath 传入 load 函数
[…]
}

__int64 __fastcall RadiusExtension::Load(RadiusExtension *this, const unsigned
__int16 *uncpath)
{
[…]
FileNameFromPath = ExtractFileNameFromPath(uncpath);
  v6 = FileNameFromPath;
  v7 = -1i64;
  do
    ++v7;
  while (FileNameFromPath[v7]);
  v8 = (unsigned int)(v7 + 1);
  v9 = (unsigned int)(v7 + 1) * (unsigned __int128)2ui64;
  if (!is_mul_ok(v8, 2ui64))
```
```

```
    *(_QWORD *)&v9 = -1i64;
  v10 = (wchar_t *)operator new[](v9, *((const struct std::nothrow_t **)&v9 +
1));
  *(_QWORD *)this = v10;
  if ( !v10 )
    return 8i64;
  wcscpy_s(v10, v8, v6);
  LibraryW = LoadLibraryW(uncpath); // =====> 加载
[…]
}
```

在 RadiusExtensionPoint::Load 函数中 IAS extension server 会检查传入 uncpath 是否为有效的 nt path 路径，但未考虑 remote unc path 的情况，当传入路径为 \\IP\shareddirectory\dllfile 时，可加载 client 上任意 dll，最终导致 server 端恶意 dll 加载执行任意代码。

3. 漏洞演示

演示内容：利用该漏洞获取域控服务器的控制权

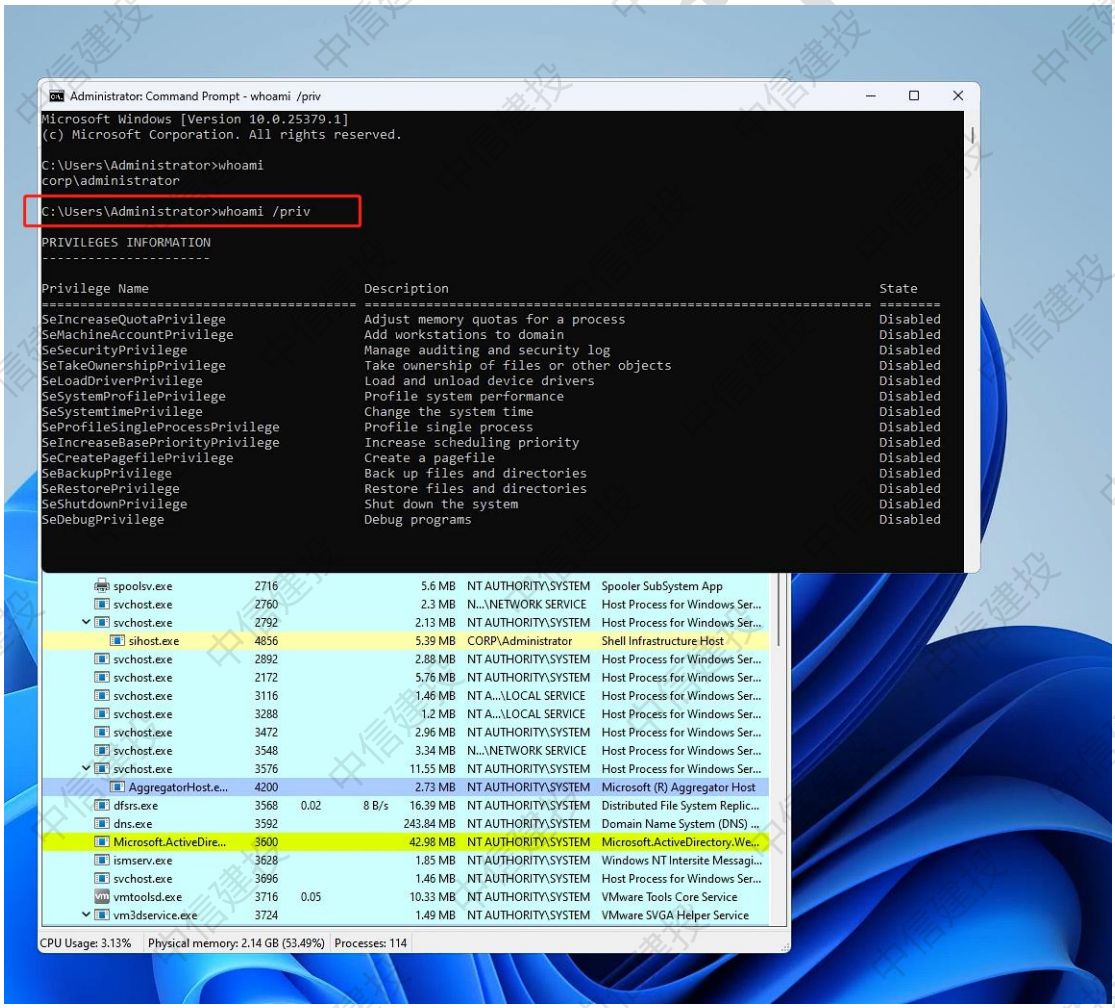
演示描述：

该演示中，（192.168.217.163）为攻击发起端，(192.168.217.129)为域控服务器，在演示中攻击发起端通过执行攻击程序 ex.exe，向域控服务器(192.168.217.129)发起攻击。

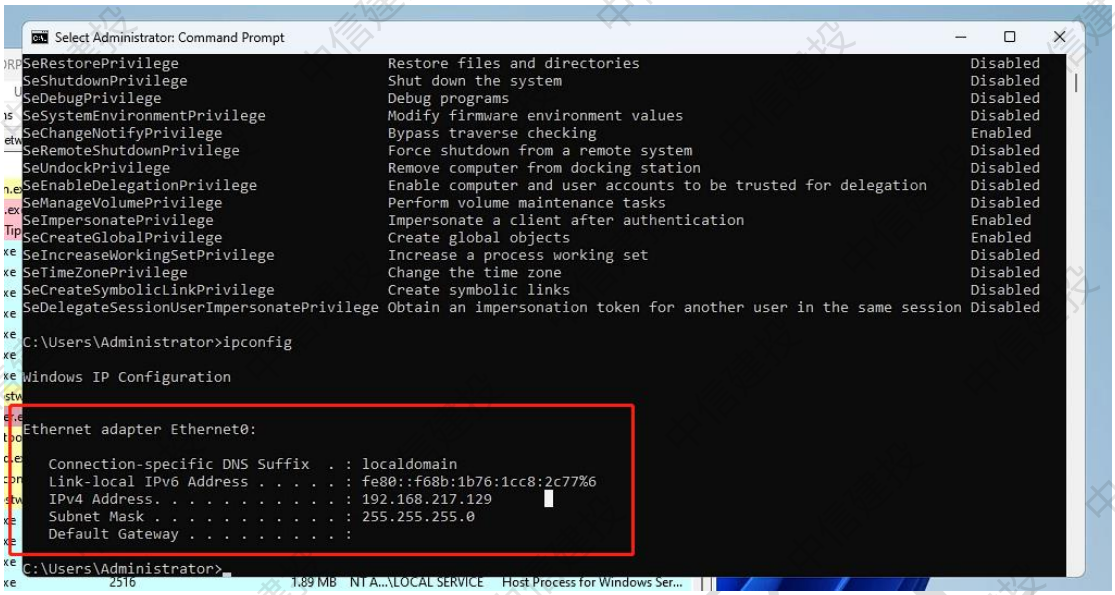
攻击者可利用该漏洞，发送经过设计构造的 Payload 报文，可在目标服务器上加载远程攻击的 DLL 文件(popz.dll)，攻击者利用加载的 DLL 文件可作为突破口可实现一系列操作，最终可直接控制域控制器。

3.1. 查看服务器当前用户的安全权限和 IP

查看域控服务器用户的安全权限

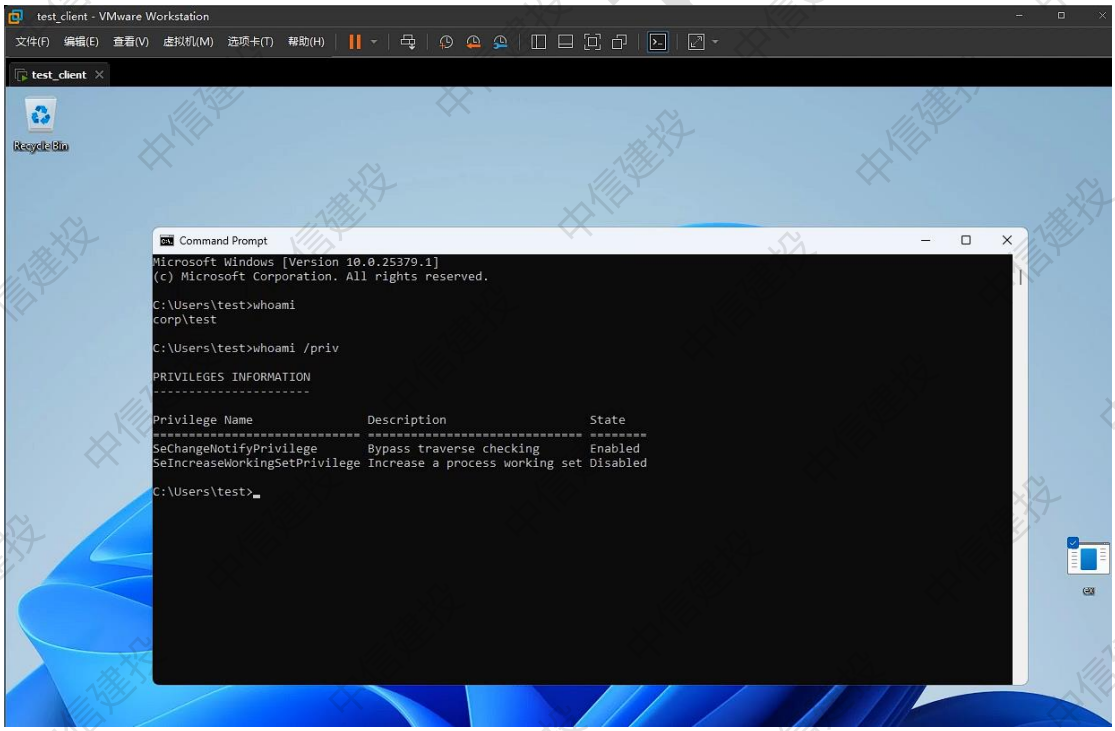


查看域控服务器的 IP 地址

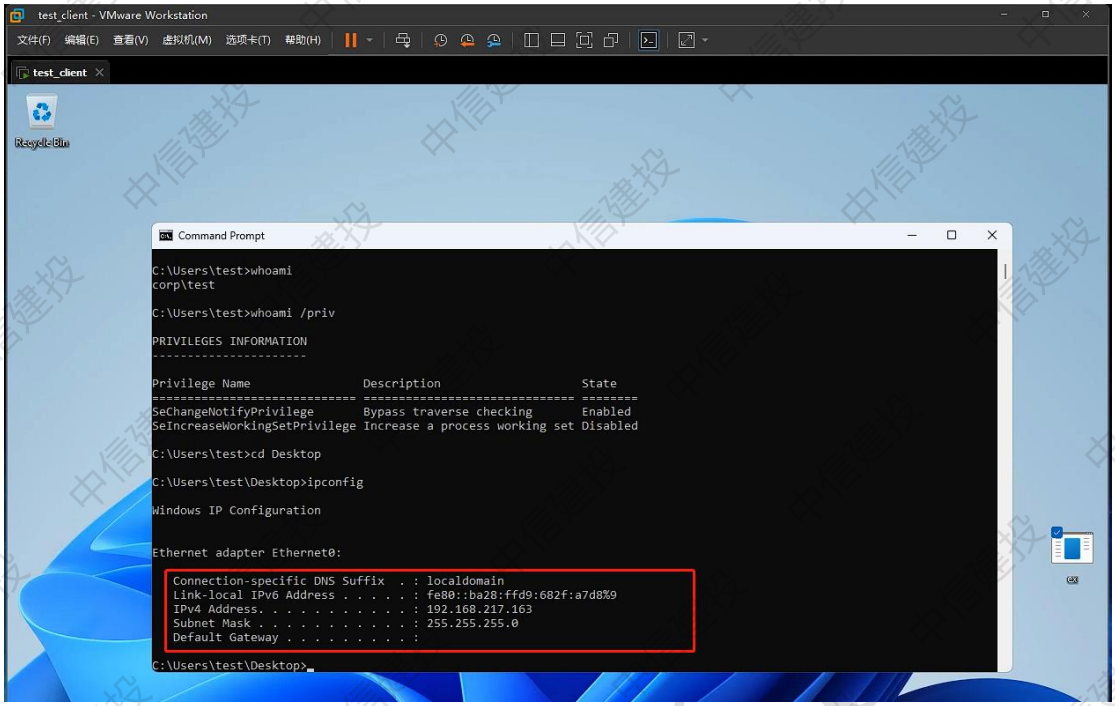


3.2. 查看客户端的安全权限和 IP 地址

查看攻击发起端的用户名和用户的安全权限

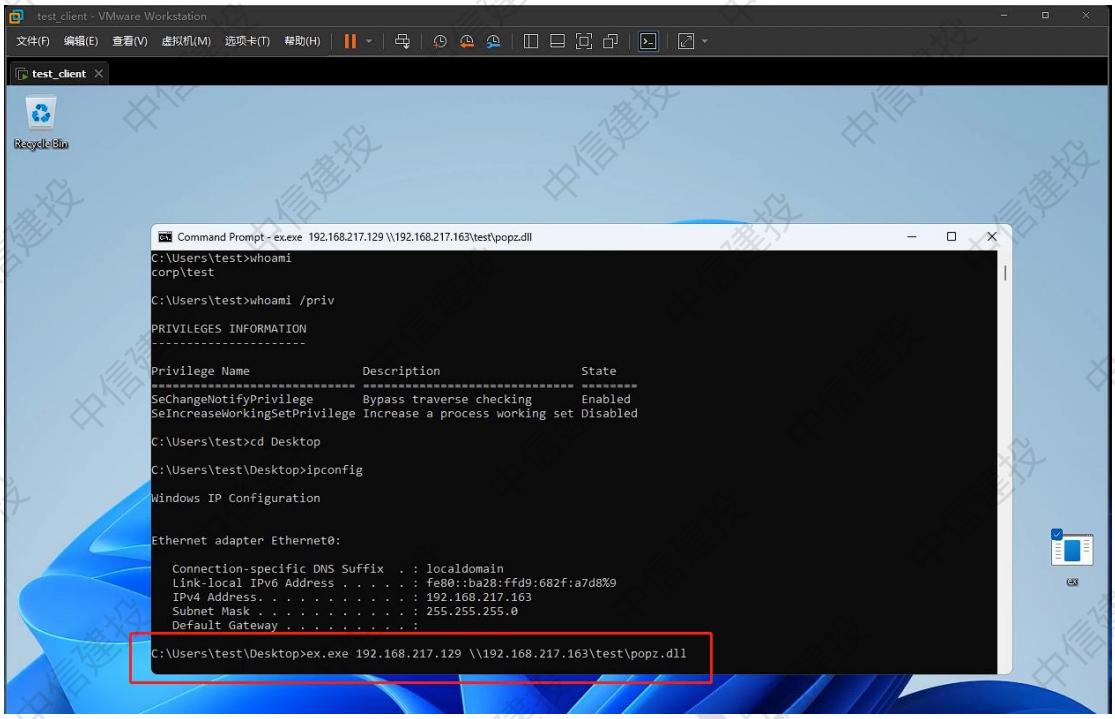


查看攻击发起端的 IP 地址

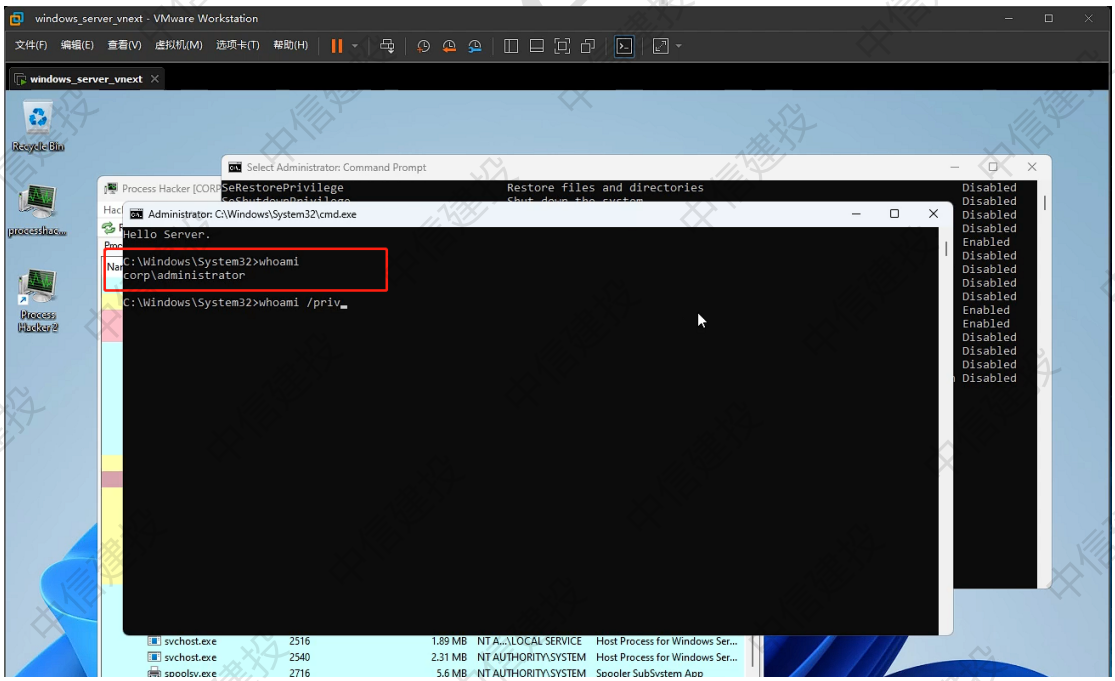


3.3. 执行 RCE 达成在服务端运行 DLL 的效果

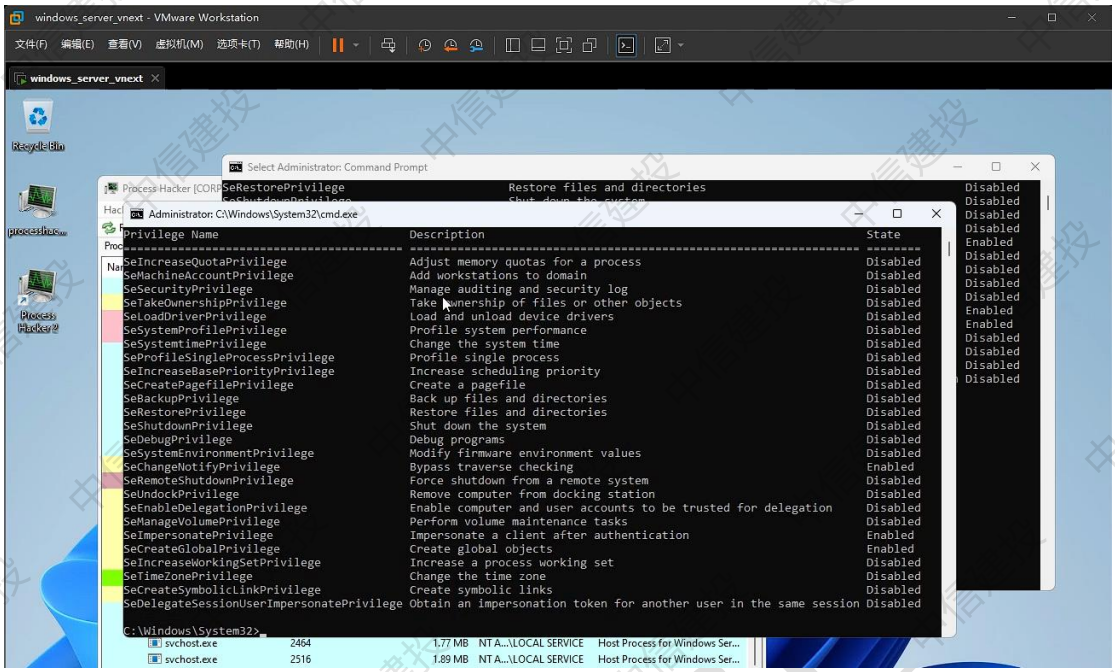
在客户端上执行并程序进行 RCE



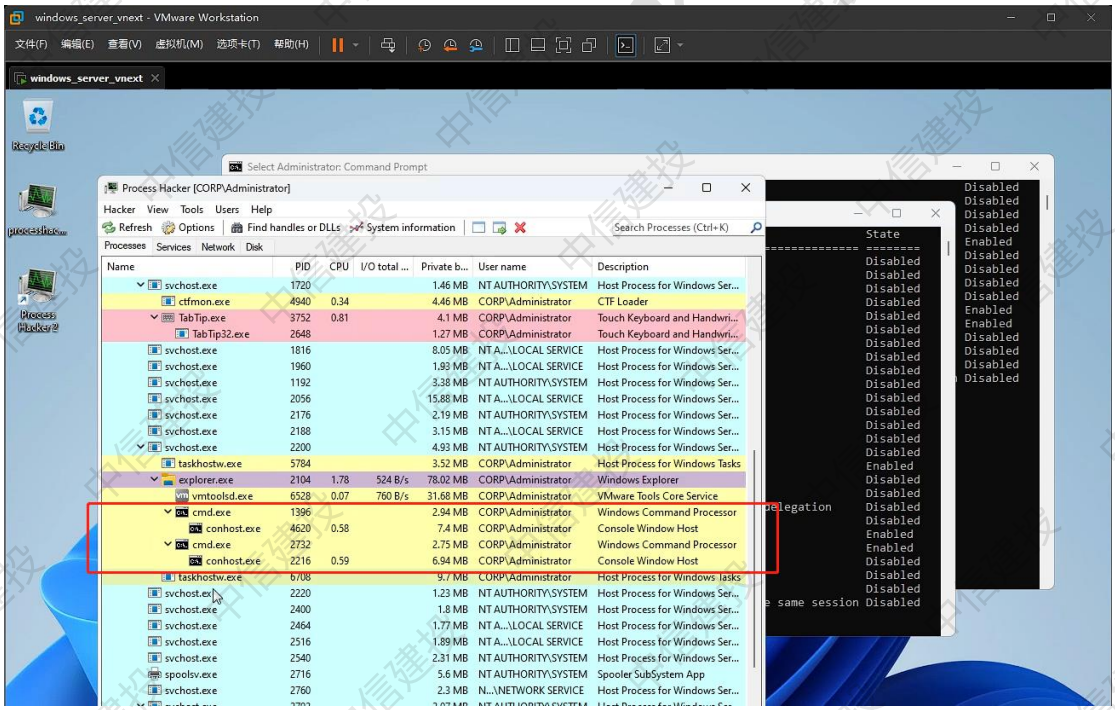
域控制器成功加载远程 DLL



远程加载成功后，弹出 cmd.exe 进程的安全权限如下(域管理员权限)：



程序执行如下：



最终效果：