## **CVE-2020-1472 域内提权**

攻击者通过NetLogon（MS-NRPC），建立与域控间易受攻击的安全通道时，可利用此漏洞获取域管访问权限。成功利用此漏洞的攻击者可以在该网络中的设备上运行经特殊设计的应用程序。

影响版本：

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Windows Server 2012

Windows Server 2012 (Server Core installation)

Windows Server 2012 R2

Windows Server 2012 R2 (Server Core installation)

Windows Server 2016

Windows Server 2016 (Server Core installation)

Windows Server 2019

Windows Server 2019 (Server Core installation)

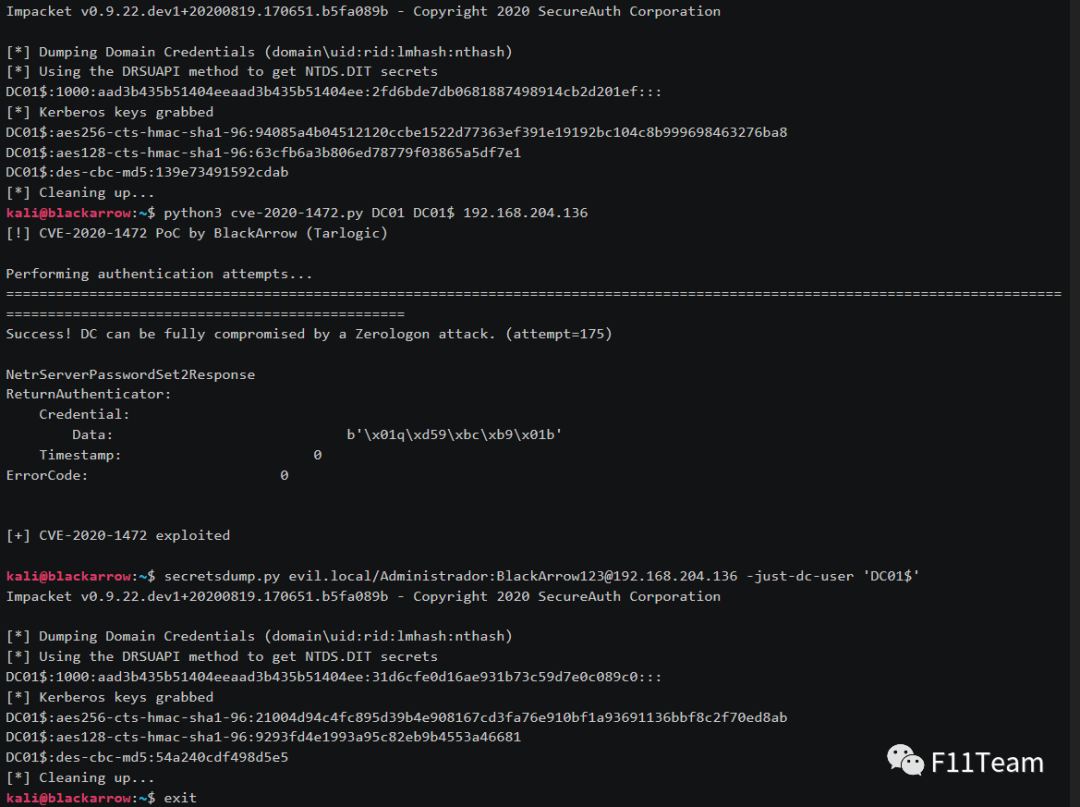
Windows Server, version 1903 (Server Core installation)

Windows Server, version 1909 (Server Core installation)

Windows Server, version 2004 (Server Core installation)

POC

https://github.com/SecuraBV/CVE-2020-1472



完整利用脚本

https://github.com/dirkjanm/CVE-2020-1472

使用：

pip install -r requirements.txt

Python zerologon\_tester.py EXAMPLE-DC 1.2.3.4