Microsoft Windows Netlogon domain authorization

CVE-2020-1472

Author:h1biki

Name_zh	Microsoft Windows NetLogon 域内提权
Name_en	Microsoft Windows Netlogon domain authorization
CVE	CVE-2020-1472
CVSS 评分	9.3
威胁等级	High
CNNVD	CNNVD-202008-548
其他 id	-----
受影响软件	Microsoft Windows

简介

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Netlogon 是一个用于为域控制器注册所有 SRV 资源记录的服务。 Microsoft Windows NetLogon 中存在提权漏洞。攻击者可借助特制应用程序利用该漏洞获取管理员访问权限。以下产品及版本受到影响：Microsoft Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016，Windows Server 2019，

Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 版本。NetLogon 远程协议是一种在 Windows 域控上使用的 RPC 接口，被用于各种与用户和机器认证相关的任务。最常用于让用户使用 NTLM 协议登录服务器，也用于 NTP 响应认证以及更新计算机域密码。

Both Microsoft Windows and Microsoft Windows server are products of Microsoft Corporation. Microsoft Windows is an operating system for personal devices. Microsoft Windows Server is a server operating system. Netlogon is a service used to register all SRV resource records for domain controllers. A privilege raising vulnerability exists in Microsoft Windows Netlogon. An attacker can exploit this vulnerability to gain administrator access via a crafted application. The following products and versions are affected: Microsoft Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 1903, Windows Server 1909 and Windows Server 2004. Netlogon remote protocol is an RPC interface used in Windows domain control, which is used for various tasks related to user and machine authentication. It is most commonly used to let users log in to the server using NTLM protocol. It is also used for NTP response authentication and updating computer domain password...

漏洞影响

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)

漏洞复现

实验环境

准备两台虚拟机

Windows Server 2008 R2 64 位　　192.168.160.131

Windows 10　　10.70.42.11

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

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

恢复原 HASH：https://github.com/risksense/zerologon

接下来利用这两台主机进行试验

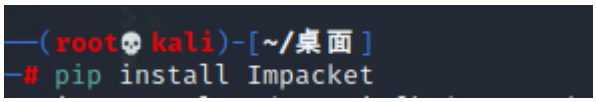
首先我们这里需要用到 python 的一个 impacket 库，下载链接如下：

https://github.com/SecureAuthCorp/impacket.git

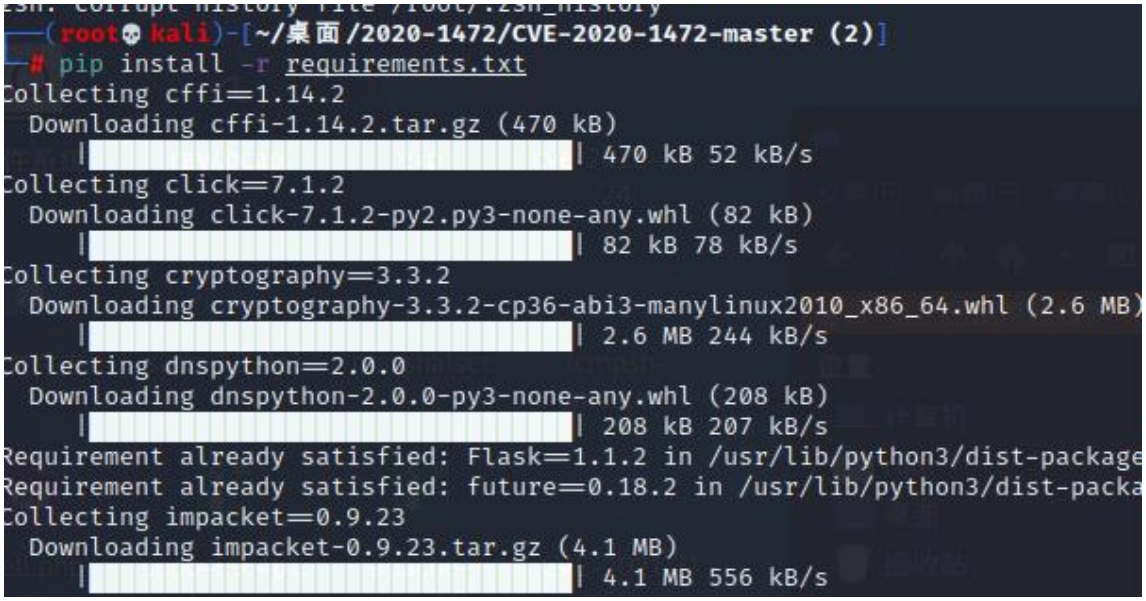
简单介绍下 impacket 库：

Impacket 是一个 Python 类库，用于对 SMB1-3 或 IPv4 / IPv6 上的 TCP、UDP、ICMP、IGMP，ARP，IPv4，IPv6，SMB，MSRPC，NTLM，Kerberos，WMI，LDAP 等协议进行低级编程访问

也可以用 pip install 在 kali 上下载，



然后下载我们的 poc 验证,在那之前我们需要先下好我们的依赖、



我们 DC 的主机名为 WIN-9MGH23RCNPB　ip 是 192.168.160.131

Poc 的使用语句如下

python3 zerologon_tester.py 域控主机名 域控 IP

exp 如下:

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

还是下载解压后放入 kali 执行如下语句:

python3 cve-2020-1472-exploit.py 域控主机名 域控 IP

这是我们的 DC 信息

漏洞触发

修改文件 impacket.dcerpc.v5.nrpc

需要利用

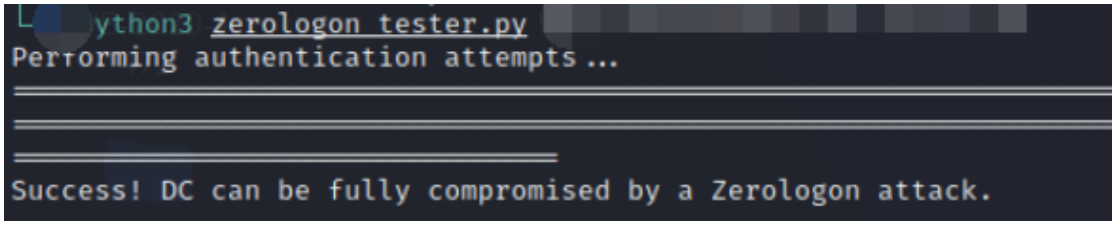
https://github.com/SecureAuthCorp/impacket/edit/master/impacket/dcerpc/v5/

nrpc.py 文件替换本机上的 nrpc 文件。本机 nrpc 文件存储路径为：

C:\Users\Administrator\AppData\Local\Programs\Python\Python38\Lib\site-

packages\impacket\dcerpc\v5\nrpc.py

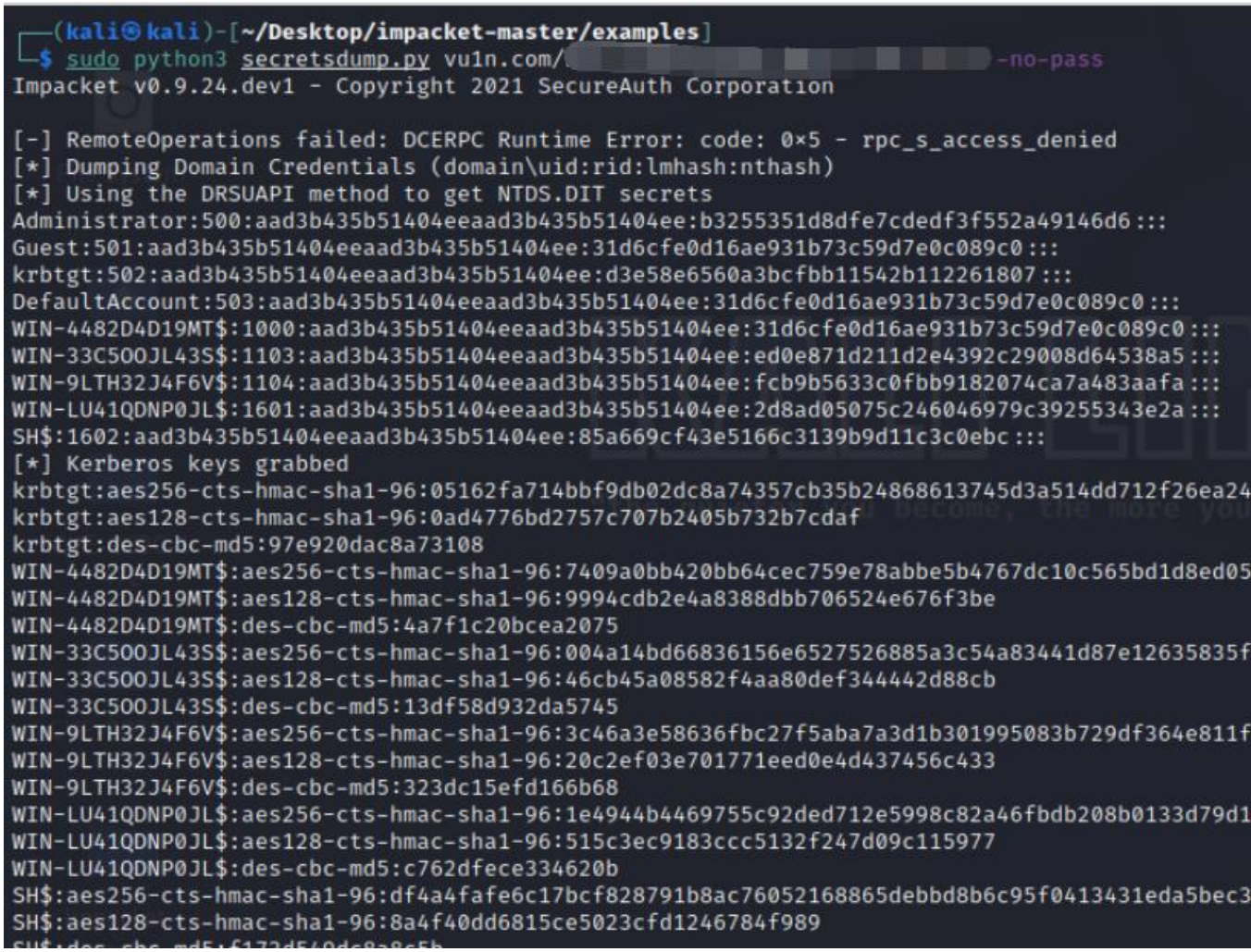
先启动我们 poc



如果有漏洞的话会显示如上内容

如果已经安装了补丁会显示攻击失败

随后我们使用 exp 置空 DC 密码，获取域内所有用户 hash

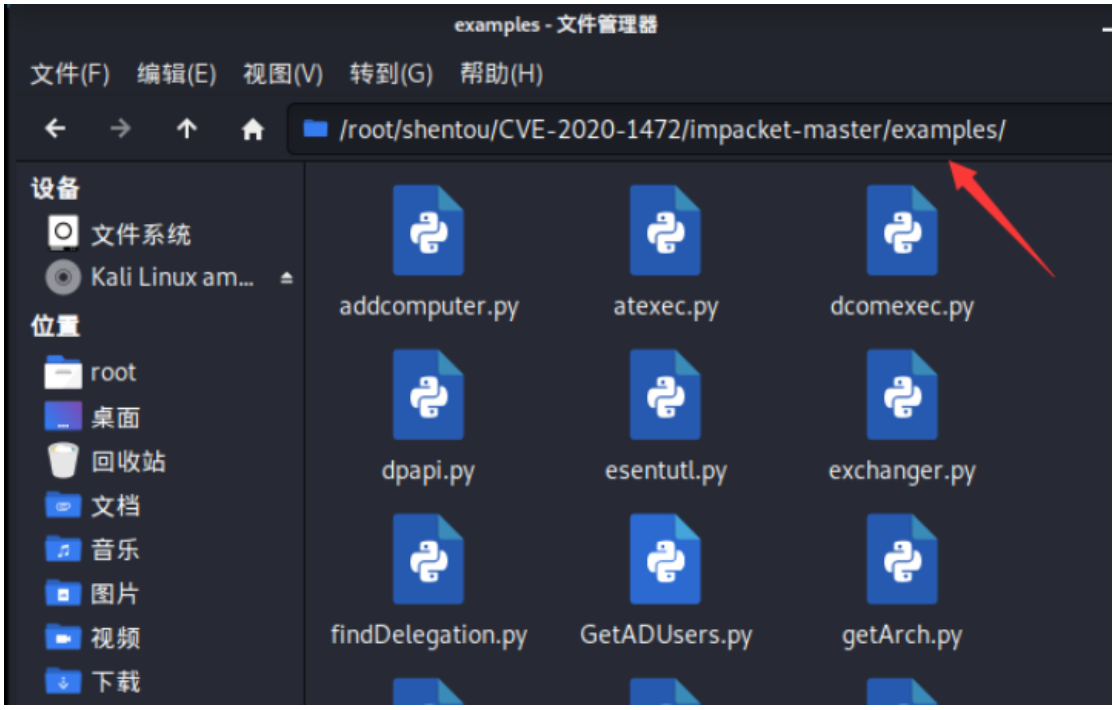


出现如下语句便是已经成功将域控打空

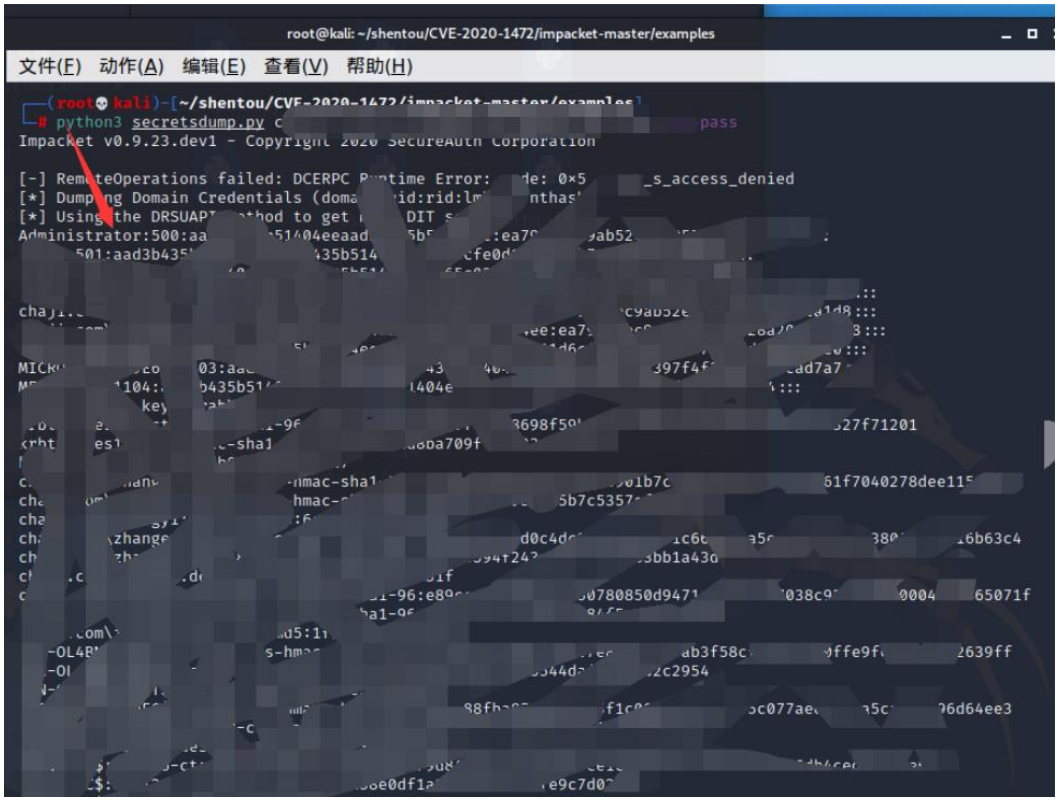
下一个步骤是用空密码 dump 域控上的 hash

首先找到之前下载的 impacket 的文件夹，找到 examples 文件夹进入，在 examples 文件夹下打开命令行，然后使用如下语句即可：

python3 secretsdump.py 域名称/域控主机名$@域控 IP -no-pass



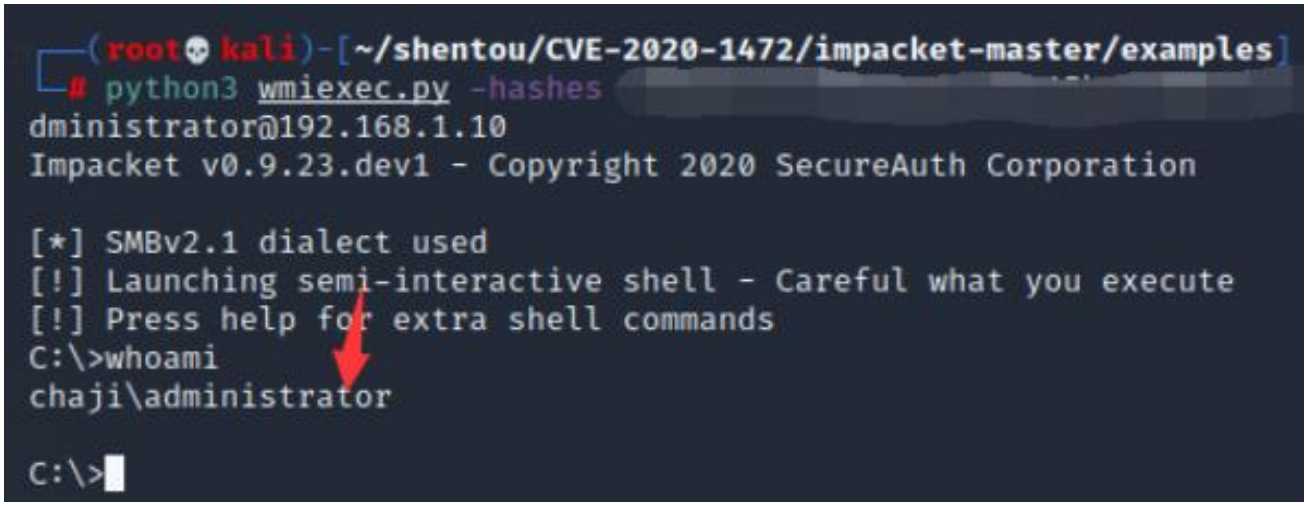
找到 administrator 的 hash 值将其复制（注意只要冒号后面的）



利用获取到的管理员 hash 通过 dos 命令远程控制域控服务器

进入之后 whoami 查看权限，为 Administrator 权限

python3 wmiexec.py -hashes hash 值 域名称/域控用户名@域控 ip



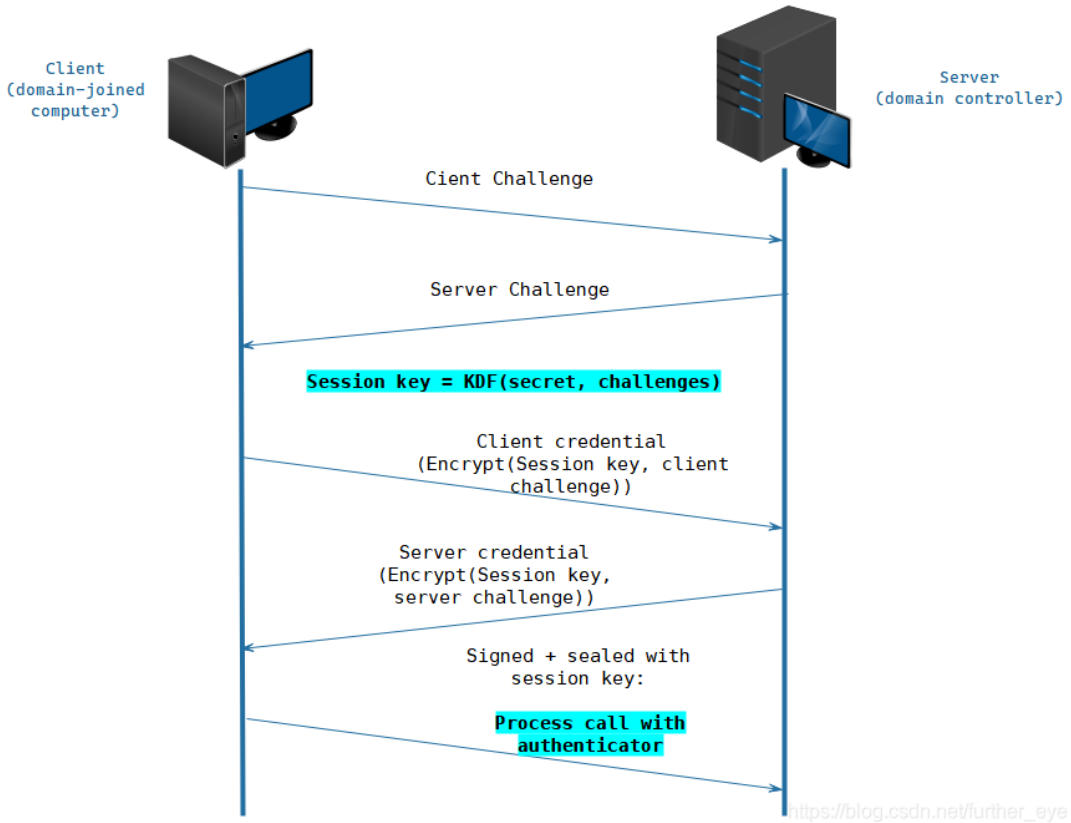
总结一下:

查看版本 -> poc 查询 -> exp 打空域控 -> 获取 hash -> 空密码 dump 域控

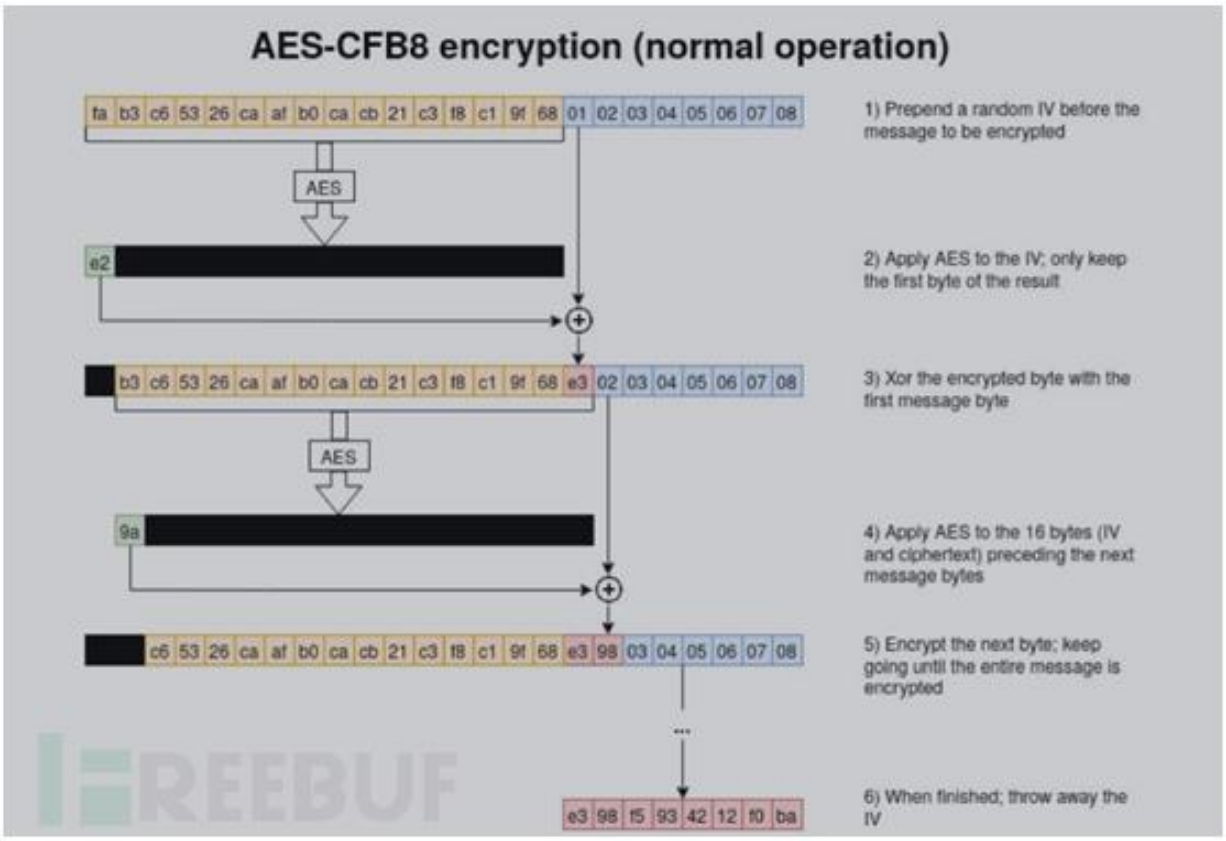
hash -> 拿到 shell

漏洞分析

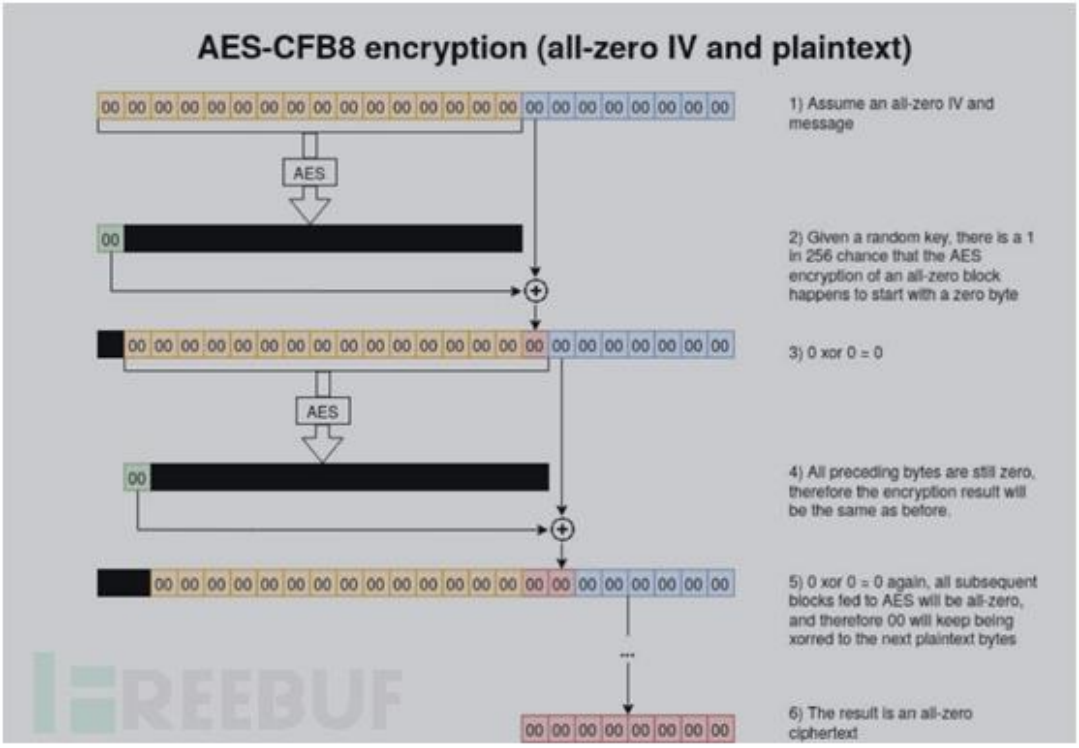
Netlogon 协议是微软提供的一套域访问认证协议，不同于大部分 rpc 服务，该协议使用的并不是典型的微软认证方式如 NTLM\Kerberos, 该协议的通信流程如下:



攻击者可控的因素有 client challenge,攻击者将它设置为全 0, server challenge 在每一轮认证过程中都会变化，secret 对应于用户密码的 hash，Encrypt 的过程采用的是 AES-CFB8



黄色部分内容即为 IV,微软错误的将其设置为全 0，而实际上为了保证 AES 算法的可靠性该部分内容应该随机生成，黄色部分后紧接着的蓝色部分为明文，对应于 client chanllenge,该部分内容攻击者可控，设置为全 0，AES 使用的 key 是将 secret、chanllenges 进行运算后得到的值，也就是说，key 会随着每一轮 server chanllenge 的变化发生变化，那么如果 IV 和 client chanllenge 为全 0 的话，那么整个 AES 运算过程变成如下所示：



在第一轮 AES 运算过程中，密文(黑色部分)第一个字节为 0 的概率是 1/256，这是因为一个字节有 8 位，全为 0 的概率是 1/256，那么由这运算得到的密文第一个字节 0x0 和 IV 以及后面全 0 的 client chanllenge 计算后得到的新一轮”明文”依旧为全 0，同样进行 AES 运算，由于第二轮运算时明文 密钥和第一轮都一致，那么这一轮所产生的密文第一个字节也同样时 0，接下来几轮计算原理以此类推，所以每一次连接都是由 1/256 的概率产生一个全 0 的密文，最理想的情况即是 256 次就一定能完成碰撞。因此 Client challenge 设置全 0 后，客户端凭据(8 字节)通过验证的概率就从 1/2^64 提高到了 1/256。

通过上述碰撞方法，攻击者便完成了域身份认证，在接下来的攻击过程用类似的方法也 bypass 了对 call 的校验，最后通过相关调用完成对域控密码的修改。值得注意的是由于整个碰撞过程中 session key 一直是未知的，攻击者可以通过 NetrServerAuthenticate3 设置合适的 flag 使得剩下的通信过程不使用 session key

进行加密。

一言以蔽之，Netlogon 协议身份认证采用了挑战-响应机制，其中加密算法是 AES-CFB8，并且 IV 默认全零，导致了该漏洞产生。又因为认证次数没做限制，签名功能客户端默认可选，使得漏洞顺利被利用

修复建议

1.进行 Windows 版本更新并且保持 Windows 自动更新开启，也可以通过下载下面链接中的软件包，手动进行升级

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-147

2.开启的 DC 的强制模式，具体可参考下面的链接进行操作

https://support.microsoft.com/zh-cn/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc