Windows下的密码hash——Net-NTLMv1介绍

wilsonlee1 / 2018-03-22 14:46:22 / 浏览数 15730

Windows下的密码hash——Net-NTLMv1介绍

0x00 前言

在之前的文章《Windows下的密码hash——NTLM hash和Net-NTLM hash介绍》分别对NTLM hash和Net-NTLMv2 hash做了介绍，对于Net-NTLMv2的上一个版本Net-NTLMv1，在安全性上相对来说更脆弱，具体脆弱在哪里呢？本文将要进行介绍

0x01 简介

本文将要介绍以下内容：

- Net-NTLMv1的加密方法
- Net-NTLMv1的破解思路
- Net-NTLMv1的利用思路

0x02 Net-NTLMv1的加密方法

对比Net-NTLMv2，Net-NTLMv2的加密流程如下：

1. 客户端向服务器发送一个请求
2. 服务器接收到请求后，生成一个16位的Challenge，发送回客户端
3. 客户端接收到Challenge后，使用登录用户的密码hash对Challenge加密，作为response发送给服务器
4. 服务器校验response

Net-NTLMv1的加密流程如下：

1. 客户端向服务器发送一个请求
2. 服务器接收到请求后，生成一个8位的Challenge，发送回客户端
3. 客户端接收到Challenge后，使用登录用户的密码hash对Challenge加密，作为response发送给服务器
4. 服务器校验response

两者的流程相同，但加密算法不同，Net-NTLMv1相对脆弱

Net-NTLMv1 response的计算方法比较简单，方法如下(目前LM hash很少接触，不考虑)：

将用户的NTLM hash分成三组，每组7比特(长度不够末尾填0)，作为3DES加密算法的三组密钥，加密Server发来的Challenge

详情可参考：

http://davenport.sourceforge.net/ntlm.html#theNtlmResponse

0x03 Net-NTLMv1的破解思路

1、捕获Net-NTLMv1数据包，提取关键数据，使用hashcat进行字典破解

服务器：

- 系统： Server2008 x64
- IP： 192.168.62.144
- 登录用户名： log1
- 登录密码： logtest123!

客户端：

- 系统： Win7 x64
- IP： 192.168.62.137

修改注册表开启Net-NTLMv1:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ /v lmcompatibilitylevel /t REG_DWORD /d 0 /f
```

注：

自Windows Vista/Server2008开始，系统默认禁用Net-NTLMv1，使用Net-NTLMv2

仅修改客户端即可，服务器不用修改

客户端通过命令行远程连接服务器，命令如下：

```
net use \\192.168.62.144 /u:log1 logtest123!
```

注：

通过界面访问\\192.168.62.144的文件共享，会多一步验证操作，使用当前用户的口令进行验证

客户端运行Wireshark，捕获数据包，如下图

前四个数据包对应NTLM认证的四个步骤

查看第二个数据包，获得Challenge，为8d2da0f5e21e20ee，如下图

查看第三个数据包，获得LM Response数据为fec9b082080e34ba0000000000000000000000000000000000，获得NTLM Response数据为51acb9f9909f0e3c4254c332f5e302a38429c5490206bc04，username为a，hostname为WIN-BH7SVRRDGVA，如下图

这里做一个对比，如果是Net-NTLMv2，Response数据多一项NTLMv2 Response，如下图

下面，使用Hashcat对该Net-NTLM v1进行破解

NTLMv1的格式为：

```
username::hostname:LM response:NTLM response:challenge
```

构造后的数据如下：

```
log1::WIN-BH7SVRRDGVA:fec9b082080e34ba0000000000000000000000000000000000:51acb9f9909f0e3c4254c332f5e302a38429c5490206bc04:8d2da0
```

Hashcat参数如下：

```
hashcat -m 5500 log1::WIN-BH7SVRRDGVA:fec9b082080e34ba0000000000000000000000000000000000:51acb9f9909f0e3c4254c332f5e302a38429c54
```

说明：

-m： hash-type，5500对应NetNTLMv1，详细参数可查表：https://hashcat.net/wiki/doku.php?

-o： 输出文件，字典文件为/tmp/password.list

–force代表强制执行，测试系统不支持Intel OpenCL

成功破解出登录的明文密码，输出如下图

2、使用Responder等中间人攻击工具，控制Challenge为固定值**1122334455667788**

可借助彩虹表还原出口令的NTLM hash

例如获得了如下NetNTLMv1 hash:

```
a::WIN-BH7SVRRDGVA:aebc606d66e80ea649198ed339bda8cd7872c227d6baf33a:aebc606d66e80ea649198ed339bda8cd7872c227d6baf33a:11223344
```

LM hash为aebc606d66e80ea649198ed339bda8cd7872c227d6baf33a

访问网站https://crack.sh/get-cracking/，使用免费的彩虹表进行破解

填入的格式如下：

```
NTHASH:aebc606d66e80ea649198ed339bda8cd7872c227d6baf33a
```

接着填入邮箱地址，提交后，在很短的时间(1分钟以内)会收到邮件，提示破解成功

参考资料：

https://crack.sh/netntlm/

如下图

破解出的ntlm hash为`d25ecd13fddbb542d2e16da4f9e0333d`，用时45秒

使用mimikatz获得该用户的ntlm hash，对比结果相同，如下图

0x04 Net-NTLMv1的利用思路

由于Net-NTLMv1的脆弱性，在控制Challenge后可以在短时间内通过彩虹表还原出用户的ntlm hash，所以在利用上首选的是将Win7环境下的默认Net-NTLMv2降级到Net-NTLMv1，获取本机的通信数据，还原出ntlm hash，实现工具: InternalMonologue

下载地址：

https://github.com/eladshamir/Internal-Monologue

通过修改注册表使Net-NTLMv2降级到Net-NTLMv1，获得正在运行的用户token，模拟用户同NTLM SSP进行交互，控制Challenge为固定值`1122334455667788`，导出返回的Net-NTLMv1 response

注：

修改注册表需要管理员权限

修改注册表开启Net-NTLMv1:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ /v lmcompatibilitylevel /t REG_DWORD /d 2 /f
```

为确保Net-NTLMv1开启成功，还需要修改两处注册表键值：

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\ /v NtlmMinClientSec /t REG_DWORD /d 536870912 /f
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\ /v RestrictSendingNTLMTraffic /t REG_DWORD /d 0 /f
```

获得的结果可以通过访问网站https://crack.sh/get-cracking/，使用免费的彩虹表进行破解，不再赘述

优点：

1. 这种方式不会对lsass.exe进程进行操作
2. 同本地NTLM SSP进行交互，不会产生流量
3. 没有进行NTLM认证，不会产生日志

补充：

如果以普通用户权限执行InternalMonologue，能够获得当前用户权限的Net-NTLMv2数据包，通过hashcat进行破解，能获得当前用户的明文口令

如上图，获得Net-NTLMv2的数据包如下：

```
a::WIN-BH7SVRRDGVA:1122334455667788:db18ac502e829dfab120e78c041e2f87:010100000000000008e2ddebb92c2d30175f9bda991833379000000000
```

使用hashcat进行字典破解，参数如下：

```
hashcat -m 5600
a::WIN-BH7SVRRDGVA:1122334455667788:db18ac502e829dfab120e78c041e2f87:010100000000000008e2ddebb92c2d30175f9bda991833379000000000
/tmp/password.list --force
```

成功破解，如下图

0x05 防御思路

自Windows Vista起，微软默认使用Net-NTLMv2协议，想要降级到Net-NTLMv1，首先需要获得当前系统的管理员权限

而对于Net-NTLMv2协议，即使抓到了通信数据包，只能对其进行字典攻击或是暴力破解，破解的概率不是很高

综上，自Windows Vista起，系统默认使用的Net-NTLMv2协议在安全性上能够保证

0x06 小结

本文对Net-NTLMv1的加密方法和破解思路进行了介绍，分析测试了工具InternalMonologue，通过InternalMonologue能在普通用户权限下获得Net-NTLMv2数据，这个

上一篇：某商城文件上传漏洞与SQL注入漏洞 下一篇：年会插曲：一个扫描3306端口传播...

1. 1 条回复

打死我也不说 2018-07-04 11:07:06

最近在看这个，发现您的文章和三好学生的好像差不多啊，你是不是三好学生啊

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板