Windows下的密码hash——NTLM hash和Net-NTLM hash介绍

wilsonlee1 / 2018-01-16 10:42:02 / 浏览数 7255 技术文章 技术文章 顶(1) 踩(0)

0x00 前言

在Windows系统中，比较常见是从系统导出来的NTLM hash，通过Hashcat能够破解出明文密码。

Hashcat支持超过200种高度优化的hash算法，其中和NTLM hash相关的有4个，分别为`NetNTLMv1`、`NetNTLMv1+ESS`、`NetNTLMv2`和`NTLM`。

NetNTLM具体是什么呢？又是如何获得的呢？本文受到byt3bl33d3r文章的启发，下面将结合自己的心得，介绍这部分内容

学习链接：

https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html

0x01 简介

- NTLM hash和Net-NTLM hash区别
- NTLM hash的加密方法
- Net-NTLM hash的破解

0x02 NTLM hash

通常是指Windows系统下Security Account Manager中保存的用户密码hash

该hash的生成方法：

1. 将明文口令转换成十六进制的格式
2. 转换成Unicode格式，即在每个字节之后添加0x00
3. 对Unicode字符串作MD4加密，生成32位的十六进制数字串

实际测试：

用户密码为`test123`

转换成十六进制的格式为`74657374313233`

转换成Unicode格式为`74006500730074003100320033 00`

对字符串`74006500730074003100320033 00`作MD4加密，结果为`c5a237b7e9d8e708d8436b6148a25fa1`

注：

MD4加密可使用工具HashCalc，如下图

下面使用mimikatz导出用户密码的hash，对比进行验证，结果相同，验证成功，如下图

在渗透测试中，通常可从Windows系统中的SAM文件和域控的NTDS.dit文件中获得所有用户的hash，通过Mimikatz读取lsass.exe进程能获得已登录用户的NTLM hash

补充：

Windows Vista和Windows Server 2008以前的系统还会使用LM hash

LM hash的生成方法本文暂不介绍

自Windows Vista和Windows Server 2008开始,Windows取消LM hash

但某些工具的参数需要填写固定格式`LM hash:NT hash`，可以将LM hash填0(LM hash可以为任意值)，即`00000000000000000000000000000000:NT hash`

0x03 Net-NTLM hash

通过是指网络环境下NTLM认证中的hash

NTLM认证采用质询/应答（Challenge/Response）的消息交换模式，流程如下：

客户端向服务器发送一个请求，请求中包含明文的登录用户名。服务器会提前存储登录用户名和对应的密码hash

服务器接收到请求后，生成一个16位的随机数(这个随机数被称为Challenge),明文发送回客户端。使用存储的登录用户密码hash加密Challenge，获得Challenge1

客户端接收到Challenge后，使用登录用户的密码hash对Challenge加密，获得Challenge2(这个结果被称为response)，将response发送给服务器

服务器接收客户端加密后的response，比较Challenge1和response，如果相同，验证成功

在以上流程中，登录用户的密码hash即`NTLM hash`，response中包含`Net-NTLM hash`

更多NTLM认证的资料可参考：

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

在NTLM认证中，NTLM响应分为NTLM v1，NTLMv2，NTLM session v2三种协议，不同协议使用不同格式的Challenge和加密算法

所以也就存在不同协议的Net-NTLM hash，即Net-NTLM v1 hash，Net-NTLM v2 hash

实际测试：

服务器：

- IP： 192.168.62.139
- 登录用户名： a
- 登录密码： test123

客户端：

- IP： 192.168.62.130

客户端通过命令行远程连接服务器，命令如下：

```
net use \\192.168.52.139 /u:a test123
```

同时，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`c0b5429111f9c5f4`，如下图

查看第三个数据包，获得客户端加密后的Challenge，为`a9134eee81ca25de`，如下图

Response数据为`a5f1c47844e5b3b9c6f67736a2e1916d:0101000000000000669dae86ba8bd301a9134eee81ca25de0000000002001e00570049004e002d00`

下面，使用Hashcat对该Net-NTLM hash进行破解

NTLMv2的格式为：

```
username::domain:challenge:HMAC-MD5:blob
```

注：

challenge为NTLM Server Challenge，domian由数据包内容获得(IP或者机器名)

HMAC-MD5对应数据包中的NTProofStr，如下图

blob对应数据包中Response去掉NTProofStr的后半部分

因此，完整的NTLMv2数据如下：

```
a::192.168.62.139:c0b5429111f9c5f4:a5f1c47844e5b3b9c6f67736a2e1916d:0101000000000000669dae86ba8bd301a9134eee81ca25de0000000002
```

为便于测试，新建字典文件，字典内容为`test123`

Hashcat参数如下：

```
hashcat -m 5600 a::192.168.62.139:c0b5429111f9c5f4:a5f1c47844e5b3b9c6f67736a2e1916d:0101000000000000669dae86ba8bd301a9134eee81
```

说明：

-m： hash-type，5600对应NetNTLMv2，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

在渗透测试中，通常有以下两种利用方法

1、使用中间人攻击的方式来获取Net-NTLM hash，常用工具为Responder和Inveigh

Responder:

python编写，可供参考的地址：

https://github.com/lgandx/Responder

Inveigh:

powershell编写，可供参考的地址：

https://github.com/Kevin-Robertson/Inveigh

实际测试：

测试环境同上，在同一网段下的一个测试主机运行Inveigh，参数如下：

```
Import-Module .\Inveigh.psd1
Invoke-Inveigh -consoleoutput Y
```

当客户端通过命令行远程连接服务器时，Inveigh捕获到Net-NTLM hash，如下图

NTLMv2
hash为a::WIN-FVJLPTISCFE:A944CF357E0938DA:C1BB2CDD038D3AA6FA53FD360D7CBA9C:0101000000000000937115D1BC8BD301033605ACA1ACA1C00000

Hashcat参数如下：

```
hashcat -m 5600 a::WIN-FVJLPTISCFE:A944CF357E0938DA:C1BB2CDD038D3AA6FA53FD360D7CBA9C:0101000000000000937115D1BC8BD301033605ACA
```

成功破解出登录的明文密码，输出如下图

2、通过多种方式强制目标客户端向伪造的服务器发起SMB连接，在伪造的服务器上捕获数据包，获得Net-NTLM hash

对于SMB协议，客户端在连接服务端时，默认先使用本机的用户名和密码hash尝试登录

实际测试：

客户端IP： 192.168.62.139

服务端IP： 192.168.62.130

服务端运行Wireshark，捕获数据包

客服端尝试连接服务器，为便于演示，通过界面操作，地址栏直接输入\\192.168.62.130，弹框提示用户名密码不正确，如下图

此时，服务端的Wireshark已经捕获到数据包，组装NTLMv2 hash，内容如下：

```
a::WIN-FVJLPTISCFE:a05179df44d8cd35:43589a30aea29cf24fbd9c01a85e4b7e:010100000000000eb8e1d9bf08ed301ca0ea89448cceba8000000000
```

Hashcat参数如下：

```
hashcat -m 5600 a::WIN-FVJLPTISCFE:a05179df44d8cd35:43589a30aea29cf24fbd9c01a85e4b7e:010100000000000eb8e1d9bf08ed301ca0ea8944
```

成功破解出客户端当前用户的明文密码，输出如下图

实际利用举例：

发送钓鱼邮件，用户打开邮件时会隐蔽访问伪造的服务器，服务器通过捕获数据包就能获得目标当前用户的Net-NTLM hash，进一步破解还原出明文密码

0x04 小结

本文介绍了NTLM hash和Net-NTLM hash的区别，实际演示NTLM hash的加密方法和Net-NTLM hash的破解方法。如果破解不出明文密码，对于NTLM hash可使用Pass-The-Hash作进一步利用，那么对于Net-NTLM hash呢？

点击收藏 | 3 关注 | 2

上一篇：Misc 总结 ----流量分析 ... 下一篇：渗透技巧——利用netsh抓取连接...

1. 2 条回复

王天 2018-01-16 11:18:34

Net-NTLM hash可以用来Pass-The-Hash哈希传递攻击吗？

0 回复Ta

wilsonlee1 2018-01-16 11:26:08

@王天 不能，但可以用来中间人攻击

0 回复Ta
