内网渗透 | 内网中的信息收集

原创 se7en HACK学习呀
2020-08-23原文

无论是通过外网打点，还是水坑钓鱼，进入内网后的第一步，也是最重要的一步就是信息收集，而且信息收集往往是一直穿插在整个内网渗透过程中。

工作组和域的区分

1.ipconfig /all 有 Primary Dns Suffix （主 DNS后缀）就说明是域内，空的则当前机器应该在工作组。2.net config workstation =工作组特征 =---------- 软件版本 Windows 10 Home China工作站域 WORKGROUP登录域 MicrosoftAccount----------
= 域特征 =---------- 工作站域 HACK7 工作站域 DNS 名称 hack7.local 登录域 HACK7----------
3.systeminfo这里注意字体大小写，工作组一般都是全大写，但是遇到的也有小写的情况，暂时不明白怎么设置的=工作组特征=----------
--------域: WORKGROUP----------
-------------= 域特征 =----------
域: hack7.local----------
-------4.net time /domain=工作组特征=----------
--------------找不到域 WORKGROUP 的域控制器。请键入 NET HELPMSG 3913 以获得更多的帮助。 ----------
=域特征=[需要域用户才能成功查询]----------
------\\DC.hack7.local的当前时间是2020/7/12 13:21:32----------

工作组内信息收集

工作组采取的一般都是常规渗透方法，因为工作组一般都是个人和少数服务器。

通常使用的方法有：扫描网段中的web服务，常用的有phpstudy，wampserver等，来寻找搭建的服务漏洞扫描开放端口信息，以及对应的服务，判断是否存在漏洞。扫描主机由于没有更新到最新版本导致的系统漏洞，比如MS17-010，补丁号为KB4013389hash抓取，hash注入，hash碰撞，口令爆破，IPC登陆，WMI，未授权访问，文件共享系统。ARP嗅探/欺骗攻击（Cain和Ettercap）DNS劫持，会话劫持。社会工程学...

本机信息收集

用户系统信息收集

1.查看当前用户权限whoami /all2.查看系统信息systeminfosysteminfo /S 192.168.1.101 /U testlab\test /P "test" 查看远程机器的系统配置3.查当前机器的机器名,知道当前机器是干什么的hostname4.查看在线用户，注意管理员此时在不在quser / query user5.查当前机器中所有的用户名，开始搜集准备用户名字典net user6.查当前机器中所有的组名,了解不同组的职能,如：IT,HR,admin,filenet localgroup7. 查指定组中的成员列表net localgroup "Administrators"8. 查询本机所有的盘符wmic logicaldisk get description,name,size,freespace /valuefsutil fsinfo drivesfsutil fsinfo volumeinfo C:|findstr "卷名" 查看卷名称，需要管理员权限9.防火墙相关netsh firewall show state 查看防火墙状态netsh firewall show config 查看防火墙配置设置防火墙日志存储位置：netsh advfirewall set currentprofile logging filename "C:\Windows\temp\FirewallLOG.log"关闭防火墙：netsh firewall get opmode disable (WIN2003之前)netsh advfirewall set allprofiles state off (WIN2003之后)允许某个程序的全连接：netsh firewall add allowdprogram C:\nc.exe "allow nc" enable (WIN2003之前)允许某个程序连入：netsh advfirewall firewall add rule name="pass nc" dir=in action=allow program="C:\nc.exe"允许某个程序外连：netsh advfirewall firewall add rule name="pass nc" dir=in action=allow program="C:\nc.exe"10. 其他set 查看当前机器的环境变量配置,看有没有我们可以直接利用到的语言环境ver 查看当前机器的NT内核版本，不弹窗winver 查看当前机器的NT内核版本,弹窗，在非图形界面不执行这个命令fsutil fsinfo drives

列出当前机器上的所有盘符net share 查看当前机器开启的共享driverquery 查看当前机器安装的驱动列表 net share public_dir="c:\public" /grant:Everyone,Full 设置共享 dir /a-r-d /s /b 找当前用户可读写目录,可能会很多

网络连接信息收集

1. 查看tcp/udp网络连接状态信息 netstat -ano 查看本机所有的tcp,udp端口连接及其对应的pidnetstat -anob 查看本机所有的tcp,udp端口连接,pid及其对应的发起程序netstat -ano | findstr "ESTABLISHED" 查看当前正处于连接状态的端口及ipnetstat -ano | findstr "LISTENING" 查看当前正处于监听状态的端口及ipnetstat -ano | findstr "TIME_WAIT" 查看当前正处于等待状态的端口及ip2.查看网络配置ipconfig /all3. 查看本地DNS缓存 ipconfig /displaydns4. 查看路由表 route print5.查找有价值的内网arp通信记录arp -a6.跟踪本机出口iptracert 8.8.8.8

软件进程信息收集

1. 查看杀毒软件 wmic /namespace:\\root\securitycenter2 path antivirusproduct GET displayName,productState,pathToSignedProductExe2.查看本机安装程序wmic product get name /valuewmic product get name,version3. 查看当前机器的进程信息 tasklist /svc 显示当前机器所有的进程所对应的服务 [只限于当前用户有权限看到的进程]tasklist /m 显示本地所有进程所调用的dll [同样只限于当前用户有权限看到的进程]tasklist /v 寻找进程中有无域管启用的进程，或者杀软进程taskkill /im iexplore.exe /f 用指定进程名的方式强行结束指定进程

历史凭证信息收集

引用自：https://github.com/klionsec/RedTeamer 批量抓取当前机器上的"各类基础服务配置文件中保存的各种账号密码"比如，各种数据库连接配置文件，各类服务自身的配置文件(redis,http basic...)... 想办法"控制目标运维管理/技术人员的单机,从这些机器上去搜集可能保存着各类敏感网络资产的账号密码表" 比如，*.ls,*.doc,*.docx, *.txt.... 抓取各类

" 数据库客户端工具中保存各种数据库连接账号密码比如,Navicat,SSMS[MSSQL自带客户端管理工具,里面也可能保存的有密码(加密后的base64)] 抓取当前系统 " 注册表中保存的各类账号密码 hash" [Windows] 抓取当前系统所有 " 本地用户的明文密码 /hash" [Windows & linux] 抓取当前系统的所有 " 用户 token" [Windows] 抓取 "windows 凭据管理器中保存的各类连接账号密码 " 抓取 "MSTSC 客户端中保存的所有rdp连接账号密码"抓取各类 "VNC客户端工具中保存的连接密码"抓取 "GPP目录下保存的各类账号密码" [包括组策略目录中XML里保存的密码hash 和 NETLOGON 目录下的某些脚本中保存的账号密码] 抓取各类 "SSH 客户端工具中保存的各种 linux 系统连接账号密码 ", SecureCRT,Xshell,WinSCP,putty 抓取各类 " 浏览器中保存的各种 web 登录密码和 cookie 信息 ",Chrome [360 浏览器],Firefox,IE,QQ 浏览器抓取各类 " 数据库表中保存的各类账号密码 hash" 抓取各类 "FTP客户端工具中保存的各种ftp登录账号密码", filezila, xftp...抓取各类 "邮件客户端工具中保存的各种邮箱账号密码", forxmail, thunderbird...抓取各类 "SVN 客户端工具中保存的所有连接账号密码及项目地址 " 抓取各类 "VPN客户端工具中保存的各种vpn链接账号密码"

用户敏感文件收集

1. 指定目录下搜集各类敏感文件 dir /a /s /b d:\"*.txt"dir /a /s /b d:\"*.xml"dir /a /s /b d:\"*.mdb"dir /a /s /b d:\"*.sql"dir /a /s /b d:\"*.mdf"dir /a /s /b d:\"*.eml"dir /a /s /b d:\"*.pst"dir /a /s /b d:\"*conf*"dir /a /s /b d:\"*bak*"dir /a /s /b d:\"*pwd*"dir /a /s /b d:\"*pass*"dir /a /s /b d:\"*login*"dir /a /s /b d:\"*user*"2. 指定目录下的文件中搜集各种账号密码findstr /si pass *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bakfindstr /si userpwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bakfindstr /si pwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bakfindstr /si login *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bakfindstr /si user *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak3. 查看，删除 指定文件 type c:\windows\temp\admin_pass.bak 查看某个文件内容 del d:\ad*.* /a /s /q /f 强制删除指定路径下的所有文件 tree /F /A D:\ >> file_list.txt 导出指定路径下的文件目录结构rd /q/s c:\windows\temp\test 删除文件夹

存活主机探测

基于icmp

```
for /L %I in (0,1,254) DO @ping -w 1 -n 1 192.168.7.%I | findstr "TTL=" >> pinglive.txt
```

扫描的话建议直接在内网进行扫描，速度和准确率都比较有保障。

常用的工具[最多10秒一个c段]：nbtscan[基于smb和netbios的内网主机发现方式]、Ladon、自开发工具socks代理扫描：goby

域内信息收集

下文仅限于域内的信息收集，均不会涉及域内认证原理等概念，后面会对windows认证方式单独写一篇总结。

net组件搜集域内信息

net user /domain 查看当前域中的所有用户名,根据用户名总数大概判断域的规模net user xingzheng /domain 查看指定用户在当前域中的详细属性信息net accounts /domain 查看当前域的域内账户密码设置策略net config workstation 查看看当前的登录域net view 查看当前域中在线的机器,不太直观,批处理把机器名对应的ip也显示出来----WIN10下使用Net view会出现如下报错System error 1231System error 6118解决：https://social.technet.microsoft.com/Forums/en-US/6f102ed1-8e76-4cb7-8dec-05714466d441/net-view-system-error-1231?forum=win10itpronetworking----net view /domain 查看所有的域名称net view /domain:domain_name 查看指定域中在线的计算机列表net time /domain 查看时间服务器，一般域控会做时间服务器net accounts /domain 查看当前域的域内账户密码设置策略net group /domain 查看当前域中的所有组名net group "domain admins" /domain 查看当前域中的域管账户net group "domain computers" /domain 查看当前域中的所有的计算机名（登录过该域的计算机）net group "domain controllers" /domain 查看域控nltest /domain_trusts 查看域内信任关系

其他补充

```
nltest /domain_trusts     查看域内信任关系dnscmd /zoneexport hack7.local
dns.txt      ※【DC执行】导出域内DNS信息nslookup -q=mx hack7.local
查看域内邮件服务器nslookup -q=ns hack7.local     查看域内DNS服务器netdom
query pdc     查看域内的主域控，仅限win2008及之后的系统
```

dsquery导出域信息

利用dsquery 工具搜集域内信息，域成员机器需要自己传上去

```
dsquery                                                    computer
查看当前域内的所有机器,dsquery工具一般在域控上才有,不过你可以上传一个dsqueryd
squery user          查看当前域中的所有账户名dsquery group
查看当前域内的所有组名dsquery subnet
查看到当前域所在的网段，结合nbtscan使用dsquery site
查看域内所有的web站点dsquery server
查看当前域中的服务器(一般结果只有域控的主机名)dsquery user domainroot -name
admin* -limit 240     查询前240个以admin开头的用户名
```

csvde导出域信息

```
如果你有一个当前有效的域用户账户及密码csvde.exe -f c:\windows\temp\e.csv -n
-s 192.168.1.100 （DC的IP） -b 域用户名 域名
域用户密码如果你可以使用域成员主机的system权限或者当前就在DC上csvde.exe -f
c:\windows\temp\e.csv -n -s 192.168.1.100（DC的IP)
```

Bloodhound/Sharphound

BloodHound以用图与线的形式，将域内用户、计算机、组、Sessions、ACLs以及域内所有相关用户、组、计算机、登陆信息、访问控制策略之间的关系更直观的展现在Red
Team面前进行更便捷的分析域内情况，更快速的在域内提升自己的权限。它

也可以使Blue
Team成员对己方网络系统进行更好的安全检测及保证域的安全性。
这里直接介绍需要在内网机器中执行的相关命令：
此工具的导出相对来说比较暴力，且目前此工具 exe
原版已经被识别并被各种杀软查杀，包括微软win10自带的杀软 Windows Defender 。

详细参考： https://www.anquanke.com/post/id/214046

SPN扫描

不同于常规的tcp/udp端口扫描，由于spn本质就是正常的Kerberos请求，所以扫描是非常隐蔽，日前针对此类扫描的检测暂时也比较少。大部分win系统默认已自带spn探测工具即：setspn.exe，此操作无需管理权限，需域内机器执行。

```
setspn -T target.com -Q */*          可完整查出当前域内所有spn
```

详细介绍：域安全-SPN扫描

http://hackergu.com/kerberos-sec-spn-search/

ldapsearch

详细介绍：渗透基础——活动目录信息的获取

https://3gstudent.github.io/3gstudent.github.io/%E6%B8%97%E9%80%8F%E5%9F%BA%E7%A1%80-%E6%B4%BB%E5%8A%A8%E7%9B%AE%E5%BD%95%E4%BF%A1%E6%81%AF%E7%9A%84%E8%8E%B7%E5%8F%96/

定位域控

查询dns解析记录

若当前主机的dns为域内dns，可通过查询dns解析记录定位域控。

```
C:\Users\xingzheng>nslookup -type=all _ldap._tcp.dc._msdcs.hack7.localDNS request timed out. timeout was 2 seconds. 服务器: UnKnownAddress: 192.168.86.109_ldap._tcp.dc._msdcs.hack7.local SRV service location: priority = 0 weight = 100 port = 389 svr hostname = dc.hack7.localdc.hack7.local internet address = 192.168.86.109
```

SPN扫描

在SPN扫描结果中可以通过如下内容，来进行域控的定位。

```
CN=DC,OU=Domain Controllers,DC=hack7,DC=loca
```

net group

```
C:\Users\xingzheng>net group "domain controllers" /domain这项请求将在域hack7.local 的域控制器处理。组名 Domain Controllers 注释 域中所有域控制器成员-------------------------------------------------------------------------DC$命令成功完成。
```

端口识别

扫描内网中同时开放389和53端口的机器。

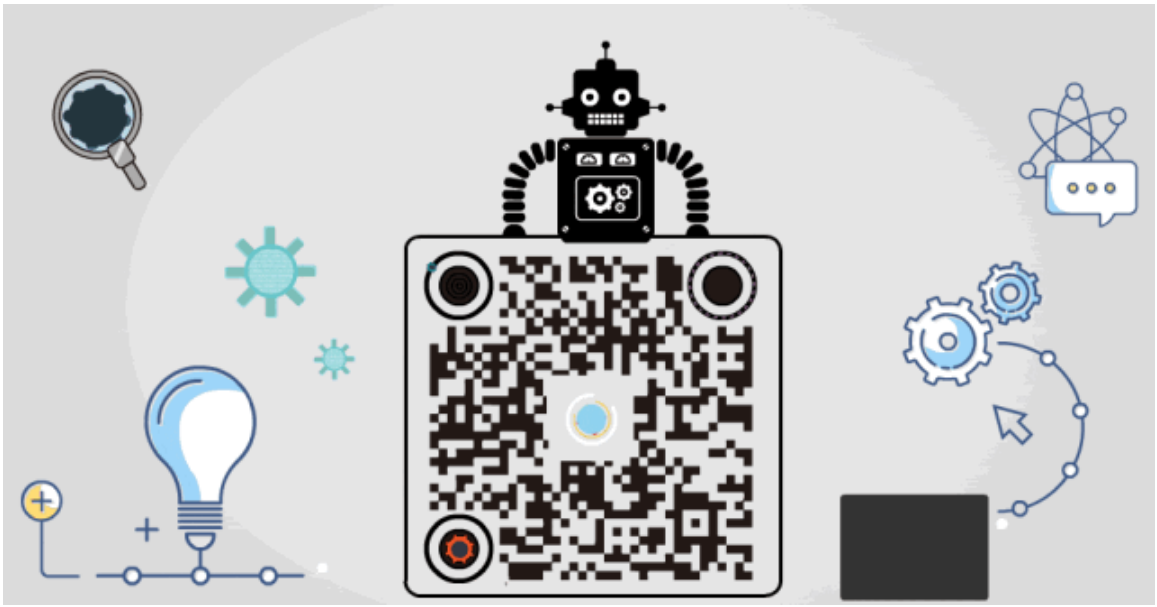
```
端口：389服务：LDAP、ILS说明：轻型目录访问协议和NetMeeting Internet Locator Server 共用这一端口。端口：53 服务：Domain Name Server（DNS）说明：53端口为DNS(Domain Name Server，域名服务器)服务器所开放，主要用于域名解析，DNS服务在NT系统中使用的最为
```

广泛。通过DNS服务器可以实现域名与IP地址之间的转换，只要记住域名就可以快速访问网站。

END

点赞，转发，在看

原创投稿作者：Se7en



精选留言

用户设置不下载评论