链滴

Netcat

作者：someone38063

原文链接：https://ld246.com/article/1548780358958

来源网站：链滴

<p><code>nc</code> 作为客户端：经常使用的参数 <code>nc -vn</cod
> （v:显示详细的连接信息，n:不进行 DNS 域名解析 ， q：退出)
先通过 <code>ping pop3.163.com</code> 获得相应的 <code>IP</code> 地址:<code>220.18
.12.110</code>,连接他的 110 端口
执行 <code>nc -vn 220.181.12.110 110</code>，服务器返回
<code>(UNKNOWN) [220.181.12.110] 110 (pop3) open</code>
<code>+OK Welcome to coremail Mail Pop3 Server (163coms[b62aaa251425b4be4eaec4ab4
44cf47s])</code>
接下来输入经过 base64 编码的邮箱账户和密码来进行登录,收发邮件
例如 <code>USER xxxx</code> <code>password xxx</code>
传输文本协议 需要其中一台服务器监听一个端口
命令： <code>nc -l -p 4444</code> l:listen p: port
另一台客户端连接到该服务器 <code>nc -vn ip 4444</code>
用于远程电子取证
传输文件
<code>A：nc -lp port >1.mp4</code>
<code>B：nc -vn ip port < 1.mp4 -q 1</code>
(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
<code>A：nc -q 1 -lp 333 <a.mp4</code>
<code>B：nc -vn ip port > 2.mp4</code>
(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
<code>A：tar -cvf - muisic/ | nc -lp port -q 1</code>
<code>B：nc -vn ip port | tar -xvf -</code>
(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
过管道进行 tar 解压)
传输加密文件
<code>A：nc -lp port | mcrypt --flush -Fbqd -a rijndael-256 -m ecb > 1.mp4</code>
<code>B：mcrypt --flush -Fbq -a rijndael-256 -m ecb < a.mp4 | nc -vn ip port -q 1 {输入密
}</code>
(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：<code>apt-get install mcrypt</code>
流媒体服务器
<code>A：cat 1.mp4 | nc -lp port</code>
<code>B：nc -vn ip port | mplayer -vo x11 -cache 3000 -</code>
(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
<code>nc -vnz ip 1-65535 (参数z：zero I/O mode [used for scanning] 扫描)</code>
<code>nc -vnzu ip 1-1024（参数u：udp协议）</code>
远程克隆硬盘
<code>A：nc -lp port | dd of=/dev/sda（of：output file)</code>
<code>B：dd if=/dev/sda | nc -vn ip port -q 1 (if：input file)</code>
(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：
<code>A：nc -lp port -c bash</code>
<code>B：nc ip port</code>
反向：
<code>A：nc -lp port</code>
<code>B：nc ip port -c bash</code>

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
<code>A：ncat -c bash --allow ip -vnl port --ssl</code>（allow 参数允许某个 IP 地址连接 ssl 加密)
<code>B：ncat -vn ip port --ssl</code>
不同平台/系统的 nc 参数功能不尽相同</p>